Programmable Modular Communication System (PMCS) Guidance Document

31 July 1997

(Revision 2)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

A. INTRODUCTION

This *Programmable Modular Communications System (PMCS) Guidance Document* provides the PMCS Systems Reference Model (SRM) and rules for its use. The PMCS SRM should be supplemented with appropriate standards from the Joint Technical Architecture (JTA). The PMCS SRM is the first step in defining the PMCS Systems Architecture intended to satisfy functional requirements to be described in a Joint Operational Architecture (JOA).

A.1 BACKGROUND AND OBJECTIVES

The rapid assimilation of leading edge information technology by the commercial market permits the government to leverage commercial items for its military and civil applications. The Department of Defense (DoD) JTA is expanding to provide necessary guidance to ensure commercial technology is leveraged across all DoD domains (C4ISR, Weapons Systems, Sustaining Base, and Modeling & Simulation). The PMCS will leverage from the expansion of the JTA in developing the communications system architecture based on the JTA standards and the development of the JOA functional requirements.

PMCS will initially base the requirements for a family of equipment on a survey of the established information exchange requirements of existing and emerging users. PMCS military and civil users are typically classified into five general domains: Airborne, Ground Mobile, Fixed Station, Maritime, and Personal Communications. The guidance contained herein begins to address the communications system architecture needed to satisfy the requirements for the various users.

The PMCS solution is to be interoperable with legacy communication systems and support growth for new requirements. It is compliant with the JTA, scaleable to match the communication requirements of different users, extendible to support growth and change, affordable over its life cycle, and uses open systems standards. Other PMCS objectives are to:

- Replace the hardware intensive designs of legacy radios by application software to accomplish waveform generation and processing, encryption, and other major communication system functions,

- Provide users the ability to dynamically change capability by reinitializing application software resident within PMCS,

- Use both common hardware and software configurations—together supporting a "plug-and-play," "mix-and-match" family of configurations—to support requirements of different users cost effectively, and

- Enable implementation of a range of capabilities from a single function communication system to an integrated multi-channel system by multiples of common hardware, different software configurations or combinations of both.

A.2 ARCHITECTURES AND REFERENCE MODELS

A.2.1 Operational, Systems, and Technical Architectures

The JTA documents formal definitions for operational, systems, and technical architectures. The definitions apply to PMCS and are:

1. Operational Architecture (OA). An Operational Architecture is "a description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges."

2. Systems Architecture (SA). A description including graphics of systems* and interconnections providing for or supporting warfighting functions (C4ISR ITF Integrated Architecture Panel, 18 December 1995). The Systems Architecture defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. It is constructed to satisfy Operational Architecture requirements per standards defined in the Technical Architecture. The Systems Architecture shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture. (C4 Chiefs Consensus System

---

* Systems: People, machines, and facilities organized to accomplish a set of specific functions (FIPS PUB 3), which cannot be further subdivided while still performing required functions.

Architecture Definition, 12 January 1996, as modified at the suggestion of the USD (A&T) community).[**]

3. Technical Architecture (TA). A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specific set of requirements. It identifies system services, interfaces, standards, and their relationships. The Technical Architecture provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

Figure 1 illustrates the relationship between the three architectures. From a PMCS perspective, the functional requirements of the JOA will provide the basic requirements for the PMCS. The environmental aspects of platforms in production and in planning that are part of the Systems Architecture determine the specific capabilities and physical characteristics of each PMCS domain. The JTA, including the standards and technical guidelines as they pertain to communications, influences the engineering specifications and common standards for the product lines that are developed for the PMCS. They also, together with the JOA functional requirements for information exchange, contribute to the PMCS Systems Architecture.

A.2.2 Reference Models

The PMCS SRM is used to develop the communications system architecture for the domain of interest. The PMCS SRM is the first step in building the PMCS Systems Architecture intended to satisfy functional requirements described in the JOA. There are two components of the PMCS SRM—an Entity Reference Model (ERM) and a Software Reference Model (SwRM). The ERM is defined by Functional Entities each bounded by a Functional Entity Interface (FEI). The SwRM defines software interfaces among the Functional Entities, as well as layered design interfaces between the software and hardware. These software interfaces are essential components of the FEIs defined in the ERM. The criterion for evolving the ERM and SwRM into a systems design is an open system approach. An open system approach achieves a technical and performance capability as an affordable solution. The structure of this document is based on the components of the SRM. The ERM is

---

[**] Interconnections: The manual, electrical, or electronic communications paths/linkages between the systems.

discussed below, while the Functional Entities and SwRM are discussed in Sections B and C, respectively.

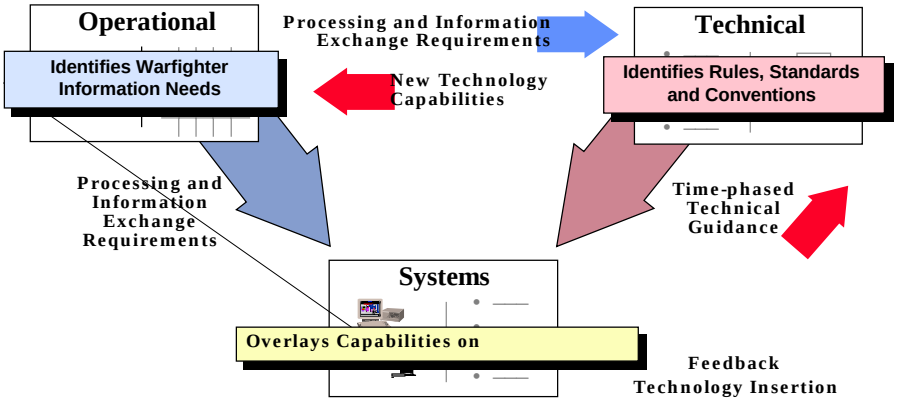


Figure 1. Architecture Relationships

A.3 PMCS ENTITY REFERENCE MODEL (ERM) COMPONENTS

This section provides an introduction to the components of the ERM. The ERM represents the minimum first order allocation of the functions of PMCS that satisfy the government goals of servicing a broad set of user needs and developing an architecture that is easily changed or upgraded. Sub-function allocation may also be beneficial to the government; however, tradeoff analyses are required to substantiate most of the initial set of sub-functions identified in the discussion of the Functional Entities in Section B.

The ERM contains eight Functional Entities where each Functional Entity accomplishes a distinct set of communication capabilities. Not all Functional Entities are required for all users. The PMCS Functional Entities and Functional Entity Interfaces (FEIs) are shown in Figure 2. Seven Functional Entities (RF, Modem, Black-Side Processes, Information Systems Security (INFOSEC), Internetworking, System Control, and Human Computer Interface (HCI)) vary in technology characteristics from the hardware intensive RF

Functional Entity to software intensive functionality of Internetworking, System Control, and Human Computer Interface (HCI) Functional Entities. An eighth Functional Entity is the split Critical System Interconnect (CSI) Functional Entity; a Black interconnect and a Red interconnect to meet the requirement for National Security Agency (NSA) endorsement. The ERM is not intended to dictate a specific packaging implementation provided independence is maintained to facilitate achieving the necessary PMCS attributes of scalability, extendibility, and affordability. Scalability relates to the ability to support the addition of existing functions (quantitative growth); whereas, extendibility pertains to the ability to support new functions (qualitative growth).

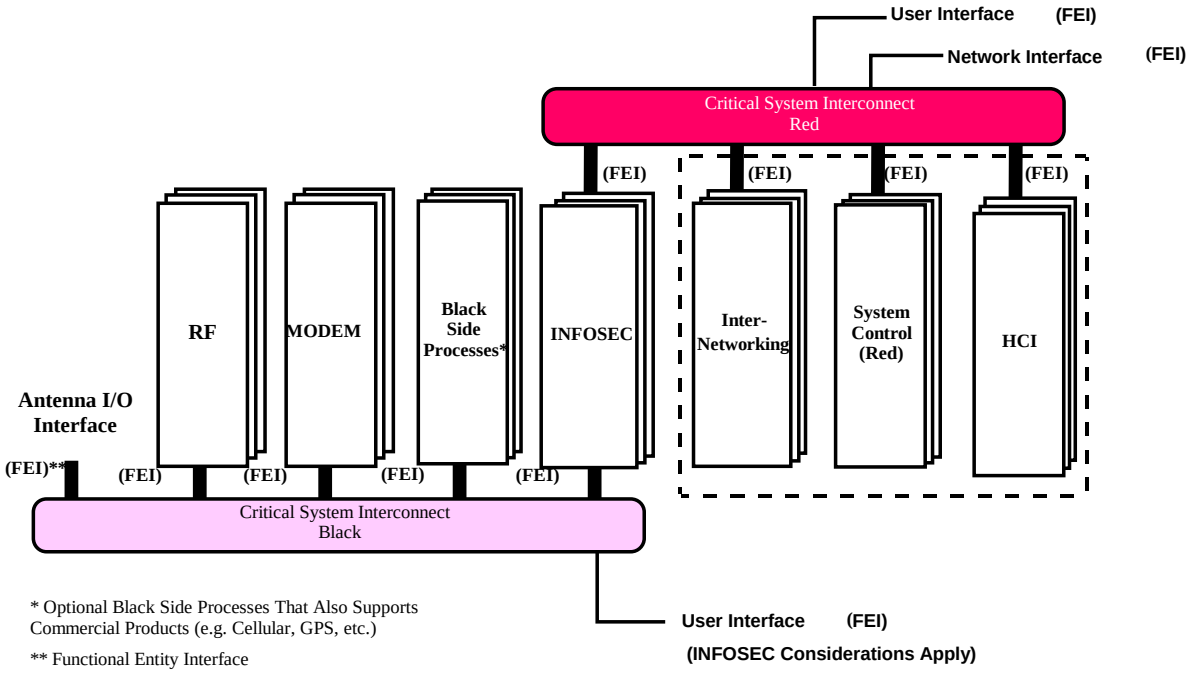


Figure 2. PMCS Entity Reference Model

The partitioning accommodates unique requirements of PMCS. The RF front end requires special design considerations compared with the rest of the system and the RF boundary reflects a transition from the analog domain to the digital domain.

The Black-Side Processes Functional Entity provides black-side networking and accommodates currently available commercial equipment that provides a specific function at an affordable price. The PMCS allows for incorporation of these products as-is or with minor changes, where practical and cost-effective. Examples include Global Positioning System (GPS), cellular telephone and Personal Communication System (PCS).

The INFOSEC Functional Entity requires special consideration due to the emerging and broadening understanding of this discipline. In the PMCS ERM as shown in Figure 2, the INFOSEC Functional Entity represents the demarcation between "Black" and "Red" information for PMCS applications that require communications security protection. In some applications, information will be protected (encrypted) at its source of generation and not require additional transmission protection (encryption). In other applications, e.g., civil aviation, communications must remain in the clear (unencrypted) at all times by international law. In the broader information–centric understanding of INFOSEC, information security functions must be viewed from a system perspective and hence may appear distributed throughout the PMCS system to insure overall protection.

The capability to support multiple, simultaneous communication channels is also illustrated in Figure 2 by multiple Functional Entities. This is not intended to imply hardware and software implementation concepts, but is only to illustrate that multiple independent channels are envisioned. A Functional Entity can consist of one or more hardware modules. Entities that are accomplished through software may coexist on a single hardware module. Each will accept initialization with software for various communication waveforms.

A.3.1 Criteria for Functional Entity Interfaces (FEI)

The FEIs identified in the ERM represent physical, electrical, logical and timing interfaces needed to achieve the independence and the flexibility to change one Functional Entity without impact to any other Functional Entities. An FEI is the set of interfaces that define boundaries around Functional Entities that the government must control to meet its objectives for PMCS. Both the ERM and the SwRM identify interfaces that comprise the FEI for a particular Functional Entity. These interfaces must be implemented by using an open systems approach. An FEI includes the interfaces from the Functional Entities to the Critical System Interconnect, interfaces external to the system, and between Functional Entities as required. For example, not all users will require the same INFOSEC capabilities. Thus, an FEI is defined at the boundary of the INFOSEC Functional Entity to facilitate the implementation of PMCS configurations with different INFOSEC requirements.

FEIs do not dictate a physical implementation. Likewise, the allocation of sub-functions to a Functional Entity that is defined by its FEI boundary does not dictate a specific physical implementation. For example:

- A single Functional Entity may be packaged on multiple discrete physical modules; or

- Multiple Functional Entities or portions of Multiple Functional Entities may be packaged on a single physical module.

The significance of an FEI is that it completely defines the interface of a Functional Entity by an open systems definition, and the FEI is identified at each level of the design and implementation process with an increasing level of specificity. There is a dualism in the definition of a FEI that equates to the dualism of the PMCS SRM with respect to the ERM and the SwRM. An FEI includes the full definition of a Functional Entity within both the ERM and the SwRM.

A.3.2 Criteria for Critical Sub-Functions

Within each Functional Entity, any sub-function tentatively assessed as significantly impacting affordability, scalability, extensibility, or rapid technology insertion is identified as a Critical Sub-Function. The interfaces of Critical Sub-Functions will be controlled by use of an open systems approach in the same manner as Functional Entities. The distinction between Functional Entities and Critical Sub-Functions is that the interfaces to Critical Sub-Functions are anticipated to be put under government configuration control later in the design process (e.g., concurrent with the establishment of the Developmental Baseline at the Critical Design Review). Critical sub-functions within each of the Functional Entities are identified in Section B.

A.3.3 Criteria For Critical Interfaces

Within each Functional Entity, the primary interfaces between sub-functions of the entity and other Functional Entities or external systems are identified as Critical Interfaces. The set of Critical Interfaces comprise an essential portion of a Functional Entity's FEI; however, the FEI will also contain additional interfaces that will be important to control but aren't critical for an understanding of the Functional Entity as described in the PMCS SRM. Critical interfaces for each of the Functional Entities are identified in Section B.

A.4 THE PATH TO A PMCS SYSTEMS ARCHITECTURE

A.4.1 Industry's Role

Industry's active participation in defining the PMCS Systems Architecture is necessary. The immediate feedback needed from industry is their position on the standards that must be supplied by the government (e.g., standards applicable to INFOSEC interfaces). Next in

priority are the standards applicable to the FEIs of the PMCS SRM. As previously stated, it is anticipated that the building codes related to Critical Sub-Functions within a Functional Entity will be defined during industry's design of PMCS products.

A.4.2 Standards

The JTA is the starting point from which to select all standard interfaces. If the JTA does not have a particular standard identified, standards are selected that meet the criteria of performance, which includes size, weight, and power, and environmental constraints. The selection criteria will identify standards and guidelines determined to be critical for interoperability, implementable, and used commercially or widely used throughout the government (in cases where commercial standards are not available). As with the DoD's recent initiative to define the JTA, the standards selected for the PMCS should meet all of the following criteria:

1. Interoperability—They ensure joint Service/Agency information exchange and support joint (and potentially combined) C4I operations.

2. Business Case—There is strong economic justification that the absence of a mandated standard will result in duplicative and increased life-cycle costs.

3. Maturity—They are technically mature and stable.

4. Implementability—They are technically implementable.

5. Public—They are publicly available (e.g., open systems standards).

6. Consistent with Authoritative Sources—They are consistent with law, regulation, policy, and guidance documents.

Standards that are commercially supported in the marketplace with validated implementations available in multiple vendors' mainstream commercial products take precedence. Publicly held standards are generally preferred. International, national, and industry standards are preferred over military or other government standards.

A.5 THE OPEN SYSTEM APPROACH

The open system approach is an integrated technical and business strategy that defines key interfaces for the communication system being developed. Interfaces generally are best defined by formal consensus (adopted by recognized industry standards bodies, specifications

and standards); however, commonly accepted (de facto) specifications and standards (both company proprietary and non-proprietary) are also acceptable if they facilitate utilization of multiple suppliers. The use of de facto specifications and standards takes advantage of the fact that firms, particularly those in the commercial arena, frequently develop hardware, software and systems standards for the design and fabrication of computing, telecommunications, display, and signal processing systems. Whether interfaces are described by consensus or de facto standards, benefits only accrue if products from multiple sources are economically possible.

The open system approach can have a profound effect on the life-cycle cost of a PMCS. The government can have access to alternative sources for the key subsystems and components to construct PMCS. DoD, Federal Aviation Administration (FAA), and other agency investment early in the life-cycle is reduced since at least some of the required subsystems or components are likely to already be available, or be developed without direct investment. Production sources can be competitively selected from multiple competitors taking advantage of competitive pressures, which motivate commercial companies to reduce prices and introduce new products, developed with internal resources. The system design flexibility inherent in the open system approach, and the more widespread availability of conforming commercial products, mitigates potential problems associated with a diminishing defense-dependent manufacturing base. Finally, life-cycle costs are reduced by a long-lived, standards–based architecture that facilitates upgrades by incremental technology insertion, rather than by large scale system redesign.

An effective open system architecture will rely on physical modularity and functional partitioning of both hardware and software. Physical modularity and functional partitioning should be aligned to facilitate the replacement of specific subsystems and components without impacting others. The subsystems and components described by the system design should be consistent with the system repairable level. Subsystems and components below the repairable level will normally not be under government configuration control. Therefore, repairs below the repairable level, if required, will be by the supplier. If the hardware and software is effectively partitioned, processing hardware can be replaced with new technology without modifying application software. Additionally, application software can be modified without necessitating hardware changes.

A.5.1 Application of an Open System Approach

The system architecture should be addressed early to maximize the number of potential solutions, and thereby help reduce program cost. By developing the architecture early in a program, the specific technology used in its implementation can then be chosen as late as possible.

Open system interfaces must be managed more rigorously than in previous practice. An interface specification or standard is inherently a performance standard, is used as such by industry, and must be recognized as such in government. System partitions must not violate the interface, unilaterally extend it, or define it so that it is no longer compliant with the standard.

The open system approach facilitates the use of lower cost, high performance subsystems and components, mostly built to commercial specifications and standards. The open system approach does not imply that only consumer grade products should be used. However, some commercial environments are as demanding as military environments, and commercial products that function in these environments will also function in the military environment. In any case, for military users, all open systems designs still must meet military requirements for PMCS.

The application of the open system approach to legacy systems is less obvious but still beneficial. Legacy systems usually have size, space, power, cooling and shape factor constraints. For these systems, the open system approach can provide form-fit-function interface (F3I) solutions within existing packaging, power, and environmental constraints. In such cases the open system solution frequently requires less system resources by using newer, more efficient technologies. The open system approach is similar to F3I except that the open system approach emphasizes choosing interfaces that are broadly accepted in the marketplace to allow for as many suppliers as possible over the long term.

B. ENTITY REFERENCE MODEL FUNCTIONAL ENTITIES

B.1 RF FUNCTIONAL ENTITY

B.1.1 Functional Definition

The RF Functional Entity is one of the components resulting from a first order allocation of the functions of the Programmable Modular Communication System (PMCS), and provides the functions required for the simultaneous transmission and reception of multiple narrowband and wideband waveforms over any frequency band of interest. The functional/sub-functional breakout and typical waveforms to be implemented are presented in Figure 3.

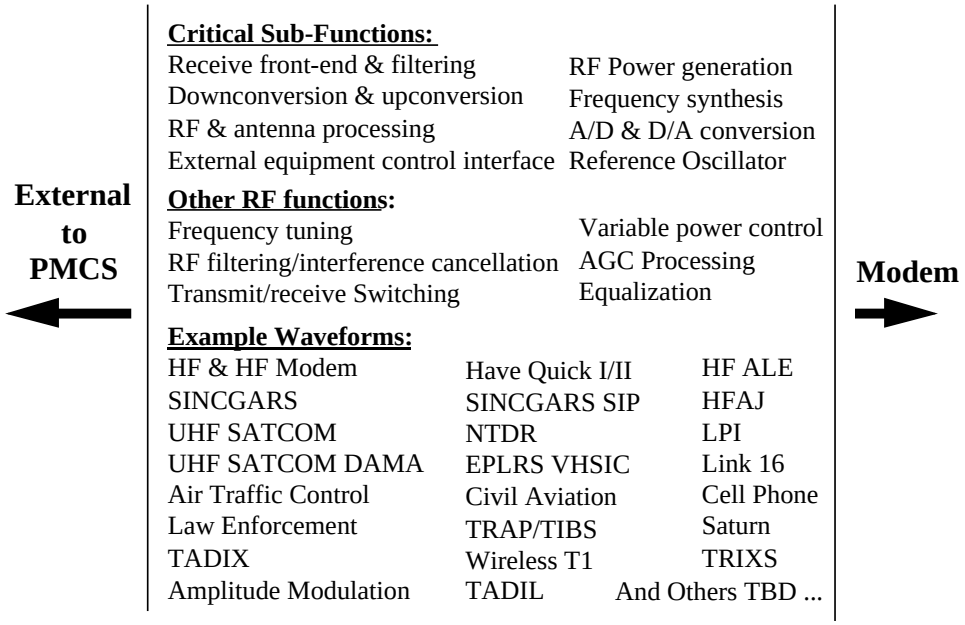


Figure 3. PMCS RF Sub-Functions & Example Waveforms

Industry is challenged to provide a functional RF Functional Entity suitable for the particular set of simultaneous communications channel waveforms a PMCS configuration is being tailored to support. In some cases, this may include multiple fixed tuned, 5 kHz channels at UHF frequencies and, in others, this may include fast hopped, wide bandwidth signals downconverted from 40 GHz. Different implementations satisfying these various needs are an acceptable cost

effective solution. The solution is also driven by environmental and mission requirements. In all cases, PMCS performance with legacy waveforms should be at least as good as legacy radio performance.

All sub-functions of the RF Functional Entity should be programmable to the extent possible. In other words, an all digital receiver/transmitter is desired. It is understood that technology will prevent such an implementation as frequency and waveform bandwidth requirements limit the digital implementation.

The implementation could accommodate direct baseband conversion, multiple frequency conversion or applicable conversions, so as to give users the flexibility of choosing a cost-effective solution for individual service/agency needs. Example waveforms are listed in Figure 3 to show the PMCS designer the complexity of the PMCS and surface the critical requirement drivers.

B.1.2 Critical Sub-Functions

Eight sub-functions are identified as potentially servicing more diverse performance requirements or changing more frequently due to technology upgrade than the others. These sub-functions are therefore currently labeled critical with the appropriate interfaces needing to be considered for control. They are:

Receive front-end and bandlimiting filtering: Various platform (cosite) requirements may require unique implementation of the same basic functions.

RF signal and power generation: Spectral containment needs (including cosite interference mitigation) may be a cost driver and require special implementations in certain applications.

Down Conversion and Up Conversion: Dependent on technology and mission requirements.

Frequency synthesis: Sophisticated waveforms (e.g., fast frequency hopped (FH)) can drive cost and may dictate low- and high-performance implementations.

RF and antenna processing: Antenna control and processing are tied to individual platform needs (beamforming, steering, nulling, etc.).

A/D & D/A conversion: Directly tied to introducing wider bandwidth waveforms.

External equipment interface: New and legacy equipment may require a different interface implementation.

Reference oscillator: Provides internal frequency reference and may require low- and high-performance implementations.

These sub-functions represent those areas where one solution might unnecessarily burden the less sophisticated user (e.g., frequency synthesis, A/D & D/A). A fast frequency hopping requirement or wide bandwidth waveform might, for instance, not be needed by the FAA's general aviation population, and consequently unnecessarily burden their implementation if only one solution were available. The challenge is to make the correct technical and business decisions and to identify which sub-functions must be segmented and which interfaces controlled to allow both user requirements to be met and cost to be controlled.

Receiver front-end and bandlimiting filtering: The main attributes include low noise amplification and pre-selection filtering. The specifications will be dictated by the mission and platform installation. The filters should provide appropriate selectivity for cosite mitigation but may need to be tunable for FH systems. Provision should be made for reception of wide-band waveforms.

RF signal and power generation: The RF signal and power generated by PMCS for transmission should be controllable and must be capable of supporting linear and non-linear waveforms with high efficiency over a broad frequency band. Tradeoffs between broadband and high power levels without burdening narrowband users is important. It must also satisfy diverse and stringent cosite or spectrum containment requirements.

Downconversion & Upconversion: This is a broadband frequency translation function in which information bearing RF signals are translated to low frequency for baseband processing and conversely, baseband signals are translated to higher frequency for transmission over the air. Many conversion mechanisms could be utilized to accomplish this function. The appropriate baseband filtering function may also be included.

Frequency synthesis: This sub-function will synthesize frequencies from a standard frequency source with appropriate resolution, spectral purity, tuning speed and stability using analog and digital techniques.

RF and antenna processing: An interface to legacy and ancillary communication equipment is contained here. Interfaces to future external communication equipment must also be addressed by this functional module.

A/D & D/A conversion: This sub-function will sample and quantize the incoming analog signal. Similarly, digital to analog converters are used to convert digital data into analog signals for radio transmission. The decision to locate the A/D and D/A converters in the RF Functional Entity instead of the Modem Functional Entity reflects the technology trend toward wider conversion, consolidation of the analog and digital conversion sub-functions (upconverter and

D/A, downconverter and A/D) to minimize the cost impact of inserting improved D/A technology, and facilitating test of the RF Functional Entity.

External equipment interface: Interfaces to external legacy and ancillary communication equipment are provided with this function.

Reference oscillator: An internal reference oscillator provides frequency reference and a time base for other entities. It may be synchronized with an external reference input.

Other RF Sub-Functions

The RF Functional Entity was further allocated into sub-functions, which included AGC processing, frequency tuning, variable power control, RF filtering/interference cancellation, equalization, RF and antenna processing, external equipment interface, and transmit/receive switching. Characteristics of these sub-functions are as follows:

AGC processing: To properly process the received signals, the signal strength must be maintained within certain limits. This sub-function will provide basic functionality plus innovation. For example, extracting weak signals in the presence of strong interfering signals, and static and dynamic calibration of communication links.

Frequency tuning: The capability to receive the frequency tuning word, decode it, and perform operations accordingly within the allocated time constraint dictated by the waveform is included in this sub-function. This information must also be provided to the RF processor for control of ancillary equipment.

Variable power control: The programmability of RF output power with specified resolution is part of this sub-function. This sub-function is necessary for both future and existing waveforms.

RF filtering/interference cancellation: Additional filtering may be necessary for selectivity or cosite mitigation.

Equalization: This sub-function provides electronic phase and amplitude balance when multiple radiating elements are used for beam forming.

Transmit/receive switching: This sub-function is necessary to provide transmit or receive selection capability.

B.1.3 Critical Interfaces

Figure 4 shows the possible RF Functional Entity critical interfaces. A brief description of each interface is provided below.

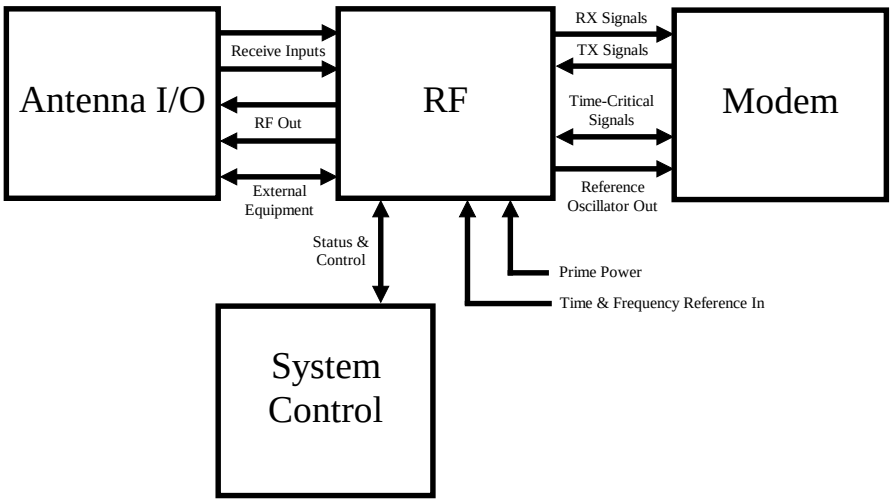


Figure 4. RF Functional Entity Critical Interfaces

Receive Inputs: These interfaces are required for connecting external receiving path elements to PMCS. Legacy platform installations may dictate these interfaces. The operating frequency may range from very low frequency to optical frequency band, but no final frequency range has been determined. Much of the existing DoD radio communications are in the HF, VHF, and UHF range, but other critical bands exist that are especially important for wideband information transfer systems.

RF Out: These interfaces are required for connecting either antennas or external transmitting path elements to the RF Functional Entity. For some implementations, the final power level may be generalized within PMCS; for others, it will not be, and an external power amplifier will be needed.

External Equipment Interface: Control of external legacy and ancillary communication equipment is provided via this interface.

Time & Frequency Reference In: This interface will allow the PMCS to receive time and frequency standards from an external source to improve the stability of internal frequency sources.

Status & Control: This is the interface that logically connects the RF Functional Entity to certain other Functional Entities such as System Control for initialization and reprogrammability, among other uses.

Time Critical Signals: This interface passes time critical signals such as the frequency tuning words for both the upconverters and downconverters, as well as other critical timing signals (i.e., hop timing, Tx/Rx switching, external equipment control, etc.). Speed and latency requirements will determine whether this is implemented by a separate physical interface than that selected for the system control.

Receive & Transmit Signal: This interface transfers digital signals between the RF and Modem Functional Entities. Speed and latency requirements will also determine whether this is implemented by a separate physical interface than that selected for the system control. This does not imply a specific implementation, and both digital and baseband IFs may satisfy the SRM..

Reference Oscillator Out: An interface must be provided to distribute Reference signals to other Functional Entities.

B.1.4 Legacy Issues

In many cases the reception and transmission of signals will require use of external legacy communication equipment and ancillary equipment such as frequency hopping multiplexers, high power amplifiers, antennas, couplers, and other items such as cosite mitigation devices for which compatible interfaces must be provided. The legacy interface requirements are diverse since both civilian and military platforms of all types are under consideration.

Interfacing with legacy communication equipment is a key issue for PMCS in order to maintain interoperability with current installed platform equipment. Migration to a more cost-effective solution, considering the life cycle cost impacts of maintaining the legacy equipment, will be a task for each program. In each case, industry will be given the opportunity to show how emerging technology in the open PMCS framework can enable migration away from the platform legacy equipment.

B.1.5 Issues for Industry to Address

There are several RF Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

- Wideband RF power generation within PMCS

A broadband power generation capability is needed to support a multitude of waveforms envisioned, but the key question is what should the minimum RF power level be? To adequately respond to this question one must answer the following questions first. What is the capability of today's technology? What is the technology trend? Is there a relationship between high power and architectural complexity or limitation?

- Performing interference cancellation internally vs. externally

  What are the pros and cons of this?

- Channel to channel RF isolation within PMCS

  Since one of the key attributes of the RF Functional Entity is simultaneous operation of multiple receivers and transmitters, a natural question is how are they isolated and to what degree?

- Open standards for RF distribution, such as fiber optic or copper for high speed digital

  Investigate the benefits of fiber optic distribution of RF after low-noise pre-amplification at the antennas. Describe your choice of interconnects and rational behind it.

- Ability of a bus to handle wideband data transfer

  How efficiently can a bus be used for transferring wideband, high-speed data between entities as a function of bus loading? What is the worst case latency? What are the EMI implications of a bus approach to high speed data transfer?

- Should a dedicated serial line be used in addition to (or instead of) a bus?

B.2 MODEM FUNCTIONAL ENTITY

B.2.1 Functional Definition

The function of the modem is to map information to and from a carrier wave for the purpose of wireless communication transmission and reception. Transmission is the mapping of voice or data signals onto a carrier for efficient transmission. Data signals may be messages, files, imagery or video. Reception is the conversion of voice or data signals mapped on a carrier to their appropriate voice or data format, effecting reception. The sub-functions necessary to accomplish this function are diverse and highly dependent on the type of communication required.

B.2.2 Critical Sub-Functions

The sub-functions in the modem may include bit or chip related operations such as interleaving, error correction coding, acquisition processing, direct sequence spreading and despreading. Also included are signal processing functions such as equalization, filtering, decimation, frequency tracking, timing recovery/bit synchronization, squelch processing, matched filtering, and various modulation/demodulation formats (AM, AM-SSB, FM, FSK, PSK, QPSK, etc.). Other anti-jam related sub-functions include Time Of Day (TOD) processing, Word Of Day (WOD) processing, request of TRANSEC bits, receipt of TRANSEC bits, frequency hopping pattern generation, and frequency tuning commands.

All sub-functions are critical from the perspective that they are likely to change with time. This is true because the modem is required to change from one mode to another to fulfill mission needs, and because communication formats and standards evolve. However, no particular sub-function stands out at this time as being susceptible to more frequent change than any other. As such, we have chosen not to require control of any internal hardware interfaces within the modem. On the other hand, the software applications that process the modulation waveforms should be independent from the hardware, since they are intended to be reusable across multiple implementations. The modulation waveform (e.g., MIL–STD–188 series) software is considered a critical sub-function in the modem.

B.2.3 Critical Interfaces

The logical interfaces between the Modem Functional Entity and the other Functional Entities are discussed below and illustrated in Figure 5.

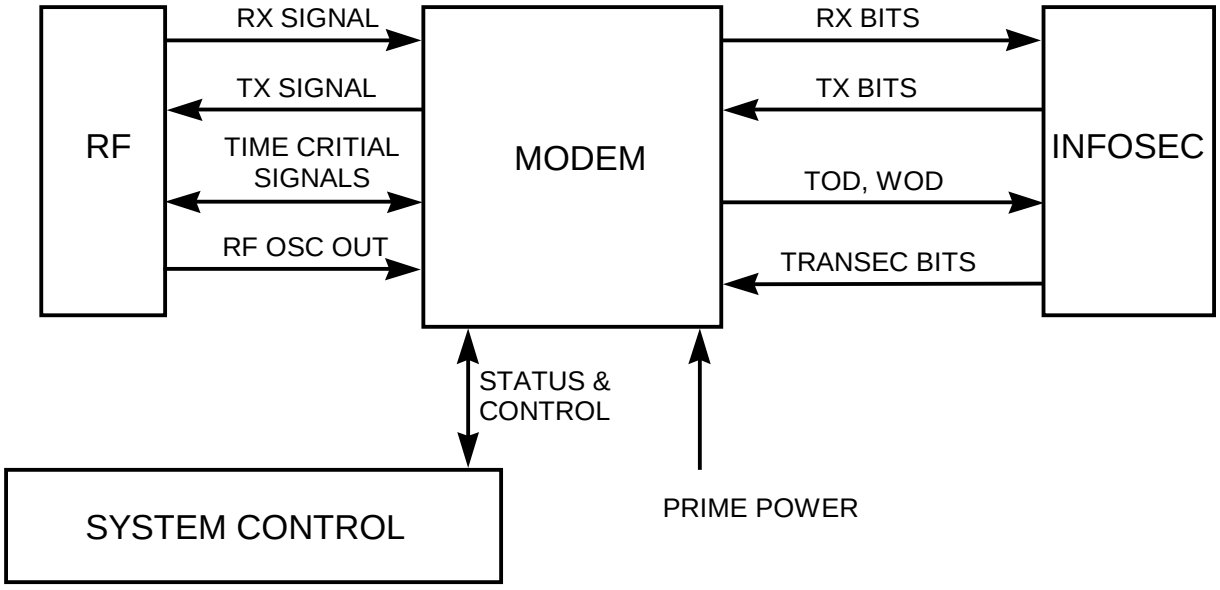


Figure 5. Modem Logical Interfaces

RF Interface: The RF interface to the modem includes the digital received signal from the RF to the modem and the digital transmit signal from the modem to the RF. This interface must also support control of the RF by the modem for parameters such as frequency, transmit/receive, transmit power control.

INFOSEC Interface: The modem provides the INFOSEC received bits for decryption and accepts encrypted bits from the INFOSEC for transmission. Seed information such as TOD, WOD, etc., is provided to the INFOSEC to support INFOSEC generation of TRANSEC bit streams. The INFOSEC provides the modem with the TRANSEC bit stream.

System Control Interface: The System Control Interface is necessary to report status information to the System Control Functional Entity. Any of the modes that are selectable are instituted by system control commands sent out as system control messages from the System Control Functional Entity to the modem and other Functional Entities. This System Control Functional Entity is also responsible for distributing new software when the modem is to be reprogrammed.

Prime Power & Timing: This interface defines the power available to the modem, the voltage(s) of this power and isolation filtering requirements between the modem and the power supply. Also included in this category are clock frequency and accuracy, plus distribution of universal radio time.

B.2.4 Modem Functional Entity Interface Standards

There are currently no widely accepted standards for the modem interface. There are modem products that incorporate a wide range of interface standards: PCI, VME, PCMCIA, PC-104, etc.

B.2.4.1 Important Interface Parameters

The primary parameters associated with interface requirements and proper interface selection are: Bandwidth, Latency, Growth Capacity, Power Consumption, Cost and Size. Bandwidth is driven by the data rate between interconnected modules and the number of modules if the interface is a bus that is shared among multiple modules. Reserve capacity for future growth also plays a role in selecting the interface. Latency is important because many of the communication processes that occur between the modem and RF are very time sensitive. If modulation waveform timing is not maintained precisely the radio cannot communicate with other radios. Cost, power consumption, and size are all interrelated parameters in the choice of an interface.

Another important interface is the messaging protocol that is used for communicating between the modem and other entities. It is desirable to use interfaces and protocols that are widely accepted so that commercial interface chips may be available to reduce the cost of interfacing a custom board into the PMCS architecture.

B.2.4.2 Modem Sub-Function Interface Standards

The critical sub-function of the modem is the modulation waveform processing application software. The interface between this software and the hardware is critical for software reuse and portability. Current modem hardware implementations range from customized ASICs and FPGAs to DSPs and CPUs. As DSPs and CPUs continue to increase in processing power, they will meet the performance needs of many more of today's modulation waveforms.

B.2.4.3 Legacy Interface Issues

Legacy interface issues are mostly driven by form factor rather than interfaces. The lack of widely accepted interface standards leaves the field open for definition. Many application areas, avionics in particular, have traditionally had a specific form factor that dictates what card sizes are acceptable, this in turn precludes certain commercial card form factor products from being compliant with the application area. This restriction may be reconsidered in PMCS.

B.2.5 Issues for Industry to Address

There are several Modem Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

The most important issue for the Modem Functional Entity is the choice of interface standards. The main components of this standard are the choice of physical interfaces and protocols used for message passing. Reuse, portability, and upgrade of modem software is also an issue. Proof of a new module's interoperability with modules from different manufacturers, especially with the large number of possible radio configurations, is a serious issue. The same is true from the software perspective, i.e., regression testing of new software on many radio configurations.

B.3 Black-Side Processes

B.3.1 Function Definition

The Black-Side Processes Functional Entity provides an insertion point for emerging functionality not yet closely associated with any one of the other PMCS Functional Entities. Unlike other Functional Entities for which the functionality is known, the Black-Side Processes Functional Entity provides standard interfaces and methods for the PMCS to accommodate new or specialized functionality. The kinds of functionality being considered include, but are not limited to:

- Commercial products such as a Global Positioning System (GPS) receiver or a cellular phone
- Bridging across two black-side channels
- Low Latency coordination
- Black-Side intra-net routing and switching
- Legacy functionality or interfaces
- Synchronization of black-side Functional Entities and external timing such as synchronization of TDMA networks with user interfaces.

The Black-Side Processes Functional Entity includes sub-functions that provide standard system control interfaces and standard electrical, mechanical and software interfaces to allow embedded commercial electronic systems and subsystems to be integrated with the PMCS. It also includes sub-functions for specialized black-side functionality that may be appropriate across a class of RF or Modem Functional Entities. The Black-Side Processes Functional Entity provides scalability and extendability for those black-side functions that would not be appropriate to allocate to the RF or Modem Functional Entities.

Interface latency can be a critical factor when the interface is part of a closed loop process such as a carrier acquisition or AGC. Latencies must be kept low enough to avoid adversely impacting the loop bandwidths. Latency can be a problem as multiple custom single-purpose interfaces are replaced by standard multi-node busses that must handle multiple signals. Overhead of the bus interfacing which may include digitization, enqueueing mechanisms, arbitration, and bridging contributes to the problem.

Commercial navigation and telecommunications equipment is available today that provides compact, highly-integrated functionality at competitive prices. Examples of such commercial equipment that could be added into the PMCS solution are GPS and Personal Communication System (PCS) including cellular telephone. The Black-Side Processes Functional Entity applies standards for incorporation of these products “as is” or with minor changes, where practical and

cost effective. The process of preparing a product for incorporation into the PMCS should be conceptually similar to, and comparable in scope with, segmenting an application for DII COE.

B.3.2 Critical Sub-Functions

In general, because the Black-Side Processes Functional Entity addresses emerging and special-purpose functionality, the ability to provide a standard control interface for commercial products is a Critical Sub-Function. In general, any sub-function provided by the Black-Side Processes Functional Entity such as low-latency control of black-side functions, is a Critical Sub-Function.

B.3.3 Critical Interfaces

The Black-Side Processes Functional Entity accommodates standard interfaces used commercial navigation and telecommunications systems. The Black-Side Processes Functional Entity provides an interface that allows a standard set of system control and monitoring functions to which commercial applications can be conformed.

B.3.4 Legacy Issues

The Black-Side Processes Functional Entity permits flexibility to accommodate modular integrated electronics in a plug-and-play fashion.

B.3.5 Issues for Industry to Address

There are several Black-Side Processes Functional Entity issues for both industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

- What criteria can be used to allocate functions to this functional entity, as opposed to the other black-side functional entities?
- What are the appropriate standard interfaces that the PMCS should accommodate?
- How should interfaces between Black-Side Processes and other Functional Entities be specified to allow flexibility (i.e., allow incorporation of not-yet-defined functionality) and also provide the standardization benefits of PMCS?

B.4 INFOSEC FUNCTIONAL ENTITY

B.4.1 Functional Definition

The Information Systems Security (INFOSEC) Functional Entity implements security services such as confidentiality, integrity, and availability to protect information being transmitted, processed, and/or stored by PMCS from unauthorized personnel. Additionally, the following three security services, access control, identification/authentication and non-repudiation, may also be required to augment the basic services. This Functional Entity may be tailored for each PMCS application, while providing for interoperability with other PMCS applications. This tailoring should be done based on the assets and/or information to be protected, the threat against those assets and/or information, and the applicable regulatory requirements. Once this has been completed and documented, an appropriate mix of technologies, policies, etc., can be identified and defined to satisfy the INFOSEC requirements for each PMCS application. The product of this tailoring effort is the definition of an Information Systems Security Policy (ISSP) for each application. In short, this ISSP documents *who* has access to *what*. Therefore, a definition of an ISSP early in the PMCS application development is essential. Our position is that industry participation—to a greater extent than ever before—is very important in the formulation of viable technologies, policies, procedures, alternative approaches to solution sets, potential implementation designs, etc.

Within the INFOSEC Functional Entity, there are three primary sub-functions.

Cryptography provides message protection through communications security (COMSEC) techniques, waveform protection through transmission security (TRANSEC) techniques, digital signature, access control, etc. These processes are executed on a special purpose, dedicated processor or trusted system hardware, whichever is appropriate.

Key management includes all activities related to cryptographic keys: key loading, over-the-air-rekey, over-the-air distribution, key selection, zeroization, etc.

Security monitoring and control serves as the "INFOSEC Conscience" of the PMCS, performing auditing of security-critical actions, supporting access control, providing black-side control, etc. We recommend that industry investigate the vulnerability of black-side control functions. Potentially significant system vulnerabilities can result from black-side control of critical system functions and/or configurations.

It should be noted that INFOSEC features and capabilities are not limited to the INFOSEC Functional Entity. Applications of the PMCS SRM and the subsequent systems architectures

must consider INFOSEC in the overall system design. Well-designed INFOSEC features and capabilities cannot compensate for a design that has not adequately considered all necessary aspects of security for a given application.

B.4.2 Critical Sub-Functions

For any classified application of the PMCS SRM, all three of these sub-functions (cryptography, key management, and security monitoring and control) are critical. For sensitive, but unclassified applications a subset of these sub-functions may be used. For each application of the PMCS, trade-offs must be made to determine the appropriate implementation of features provided by these sub-functions. To provide a measure of INFOSEC protection, security monitoring and control is recommended for all applications of the PMCS.

B.4.3 Critical Interfaces

The INFOSEC Functional Entity interfaces with the MODEM Functional Entity, the INTERNETWORK Functional Entity, the CONTROL Functional Entity, and the HCI Functional Entity. The critical interfaces are outlined in Table 1.

Table 1. INFOSEC Critical Interfaces

Interface	Input/Output	INFOSEC Subfunction	External Function
TRANSEC Time of Day/Word of Day	Input	Cryptography	MODEM
Transmit Digital Data*	Output	Cryptography	MODEM
Receive Digital Data*	Input	Cryptography	MODEM
TRANSEC Bits	Output	Cryptography	MODEM
Receive Digital Data	Output	Cryptography	INTERNETWORK

Interface	Input/Output	INFOSEC Subfunction	External Function
Transmit Digital Data	Input	Cryptography	INTERNETWORK
INFOSEC Support for Network Interface	Input/output	Cryptography, Key Management, Security Monitoring and Control	INTERNETWORK
Application Load	Input	Cryptography	CONTROL
Mode Select	Input	Cryptography, Key Management	CONTROL
Access Control	Input/output	Security Monitoring and Control	CONTROL
Key Fill	Input/output	Key Management	HCI
Key Zeroize	Input	Key Management	HCI
Cryptoalarm Indicator	Output	Cryptography	HCI
Printer Interface	Output	Security Monitoring and Control	HCI
Audit Information (i.e., information for Security Monitor)	Input	Security Monitoring and Control	ALL

* May be ciphertext or “bypassed” plaintext

B.4.4 Legacy Issues

For each application of PMCS, interoperability considerations with legacy COMSEC must be considered. As noted in other sections, the first applications of the PMCS SRM will be required to interoperate with currently fielded COMSEC equipment, while providing the

necessary flexibility to migrate to evolving cryptographic capability. These issues include cryptographic algorithm, key format (i.e., DS-102, DS-101, etc.).

B.4.5 Issues for Industry to Address

There are several INFOSEC Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

- How will industry integrate Information Systems Security Engineering (ISSE) principles into the overall design processes for the PMCS?

- How will industry incorporate trusted software design methodologies and processes for the PMCS modules, especially modules performing security critical functions? We highly recommend that industry address a trusted software development process such as the Trusted Capability Maturity Model jointly developed by NSA and the Software Engineering Institute.

- How will industry participate in the generation of an Information System Security Policy (ISSP) for each application of the PMCS architecture?

- Denial of service is a critical vulnerability to the PMCS. How will industry incorporate protection against this vulnerability into the PMCS architecture?

- How does industry plan for evolution of INFOSEC functionality from single-level security to multi-level security? There should be a phased approach: Single-Level Security initially with a migration plan to Multi-Level Security. The government will give serious consideration to creative approaches to data separation.

- Use of a special purpose processor is expected for early iterations of the cryptographic sub-function; however, are there alternate design approaches that we may not have considered?

- Are there any problems for industry participants involved in the design, development, production and/or integration of PMCS INFOSEC modules to be in compliance with the *Industrial Security Manual*?

- The reprogrammability of PMCS could require a management and security infrastructure to ensure data integrity, and configuration management to ensure hardware and software compatibility. How does industry propose to approach this?

- How to interface with GPS for timing?.

The critical point related to INFOSEC in PMCS is the common theme that links these issues together: INFOSEC must be considered from the very beginning of any PMCS effort. Addressing security issues early is cheaper in the long run, and will lead to a PMCS application that implements the necessary security services.

B.5 INTERNETWORKING FUNCTIONAL ENTITY

B.5.1 Functional Definition

The Internetworking Functional Entity provides some networking services for the RF (over-the-air) networks, host (wired) networks, and hybrid networks connected to the PMCS. These services generally include data routing, bridging, switching, link layer message processing (where necessary in support of legacy waveforms), integrated services support, and network management.

The Internetworking Functional Entity of the PMCS SRM is intended to apply in a general sense, and to encompass a wide range of networks including, but not limited to, DAMA, TDMA, circuit- and packed-switched networks.

This Functional Entity is intended to support two types of networking: Legacy and migration systems whose operation may not conform to current and future layered protocol architectures, and internetworking protocols that follow well-known commercial item architectures such as the Internet Protocol Suite or the Open Systems Interconnection Reference Model. These two sets are not disjoint; however, the government recognizes that not all legacy systems are amenable to use in a layered protocol architecture and not all military and civil aviation communication requirements can be satisfied within the constraints of a layered protocol architecture. Further discussion with industry is likely in the development of interoperable near-term and long-term solutions. (See B.5.5 below.)

In evolving to future, commercial item-based data communications, PMCS should support a full stack of internetworking protocols (as opposed to only the internetworking functions of the network layer of a protocol architecture), including link-layer and physical-layer functionality. In such an approach, new data formats and protocols, as well as certain of the legacy data formats and protocols, can be internetworked by providing a gateway layer and the associated functions. The gateway layer implements a common intermediate format that is used to encapsulate specific new and legacy data formats and protocols. An intermediate format within a layered architecture eliminates the need for specific translations between

each pair of formats and fosters the avoidance of stovepipe, monolithic communication mechanisms[†] .

It is anticipated that the Internetworking Functional Entity should be able to use commercial products that are available today and may be applicable to many of the host and RF network types. Legacy systems requiring non-internetworking support and emerging government-specific protocols that also cannot be supported via internetworking should use GFE provided software/hardware. Recognizing that internetworking is advancing rapidly in the commercial world, this Functional Entity should be flexible enough to incorporate new commercial software easily.

B.5.2 Critical Sub-Functions

There are two critical sub-functions of the Internetworking Functional Entity: RF networking and Host networking. In the event that both the RF network and the Host network use the same network protocols, these two critical sub-functions can be combined into one.

- RF networking: This sub-function includes the capabilities necessary for handling RF network protocols. For waveforms conducive to internetworking, this sub-function comprises commonly understood functionality of layered internetworking protocol architectures. For legacy waveforms that are not addressable within the scope of internetworking, services such as routing and switching or Link 16 relay, may occur on the "Black" side. In those cases, that processing would likely be partitioned as a sub-function of the Black-Side Processes Functional Entity.

- Host networking: This sub-function includes the networking capabilities necessary for communicating among systems (hosts, routers or switches, and other devices) on wired networks. For specific applications such as a handheld, Host networking may not be necessary.

B.5.3 Sub-Functions

Each of the critical sub-functions may need the following capabilities:

[†] Support of various waveforms should be modularized to, along with use of the gateway function, minimize impact of one waveforms or stack on others, and ease addition and removal.

- Routing/Switching

This refers to the functions associated with transporting formatted data (for example, an internet router or a high-speed cell switch) to the appropriate address. Quality of service, security provisions, and mobility awareness should be supported.

- Bridging

This refers to a gateway capability to tie together dissimilar channels that can greatly enhance user/mission effectiveness. This function also may provide a gateway service for legacy systems to bridge to additional capability. The number and types of bridges must be adequately defined, as well as the security requirements for such links.

- Message/Link Processing

This function is directed primarily at support of legacy protocols and emerging government-specific protocols that are not amenable to internetworking. It is associated with the networking aspects of waveforms and must accommodate existing and emerging network waveforms without adversely constraining the migration path to the future.

- Integrated Services Support

This refers to protocols and functionality for handling (primarily) time-critical data—such as digitized voice, graphics, and video—that requires specific guarantees on quality of service.

- Network Management

This refers to monitoring and control of network resources that may reside within PMCS devices or externally in attached networking devices.

Provisions and considerations related to management of PMCS-based networks in general, and RF or hybrid networks specifically, require significant investigation, development, and discussion with industry.

B.5.4 Critical Interfaces

The critical interfaces for the Internetworking Functional Entity are shown in Figure 6 (Note: this figure does not reflect interfaces not involving Internetworking). The Internetworking

Functional Entity has a control interface with the System Control Functional Entity, and data interfaces with INFOSEC and HCI entities. The following paragraphs provide a general description of the kinds of information that is exchanged. These interfaces must be further defined to specify the type of peer-to-peer information that must be exchanged between entities.

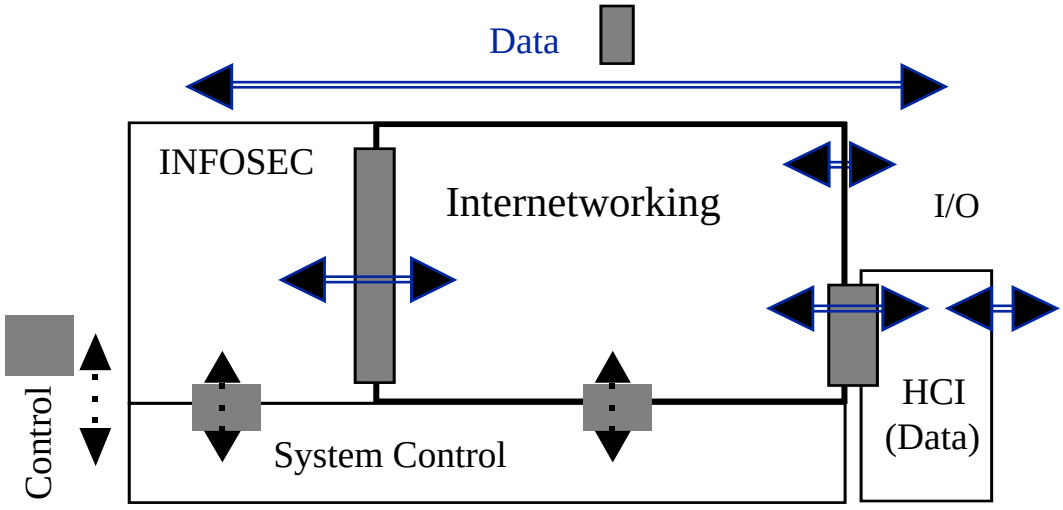


Figure 6. Logical Interfaces to the Internetworking Functional Entity

System Control Functional Entity Interface: The Internetworking Functional Entity interacts with System Control for initialization and operational parameter changes, as well as for built-in-test and system monitoring. Any such interaction must not impact the operation of other channels or networks connected to the PMCS. (Note: User control information is passed through System Control Functional Entity. Control information affecting PMCS operation received via the RF network or the host networks also is passed through the System Control Functional Entity.)

HCI Functional Entity Interface: The Internetworking Functional Entity may pass data to (or receive data from) the HCI Functional Entity. This data could have been received from (or is to be transmitted on) either the RF Functional Entity or a wired network connection.

INFOSEC Functional Entity Interface: The Internetworking Functional Entity will pass data to the INFOSEC Functional Entity for transmission on the RF network and will receive data from the INFOSEC Functional Entity that is intended for the host networks or the HCI. In addition, there may be other parameters exchanged between the two entities for support of the network interfaces. (Note: In an application that has no requirement for the INFOSEC

Functional Entity, the Modem Functional Entity will exchange data with the Internetworking Functional Entity.)

B.5.5 Internetworking Guidance

The following section provides further guidance for PMCS device internetworking functionality in the near-term and beyond. While the government recognizes that functionality of links will vary depending on the type, including whether a given type is wireline or wireless, the functionality outlined in this section is intended to apply generically to networks comprising both wireline and wireless links.

The general direction of commercial item internetworking, and so a desirable direction for PMCS internetworking as previously discussed, is towards a layered model embodied in both the seven layer ISO Open Systems Interconnection Reference Model (OSI RM) shown in Figure 7 and the Internet Protocol Suite (IPS) shown in Figure 8.

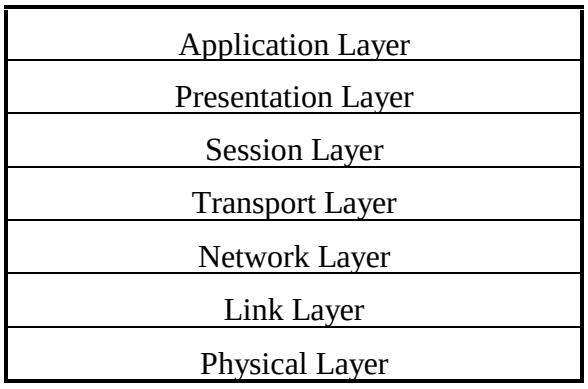


Figure 7. ISO OSI Reference Model[††]

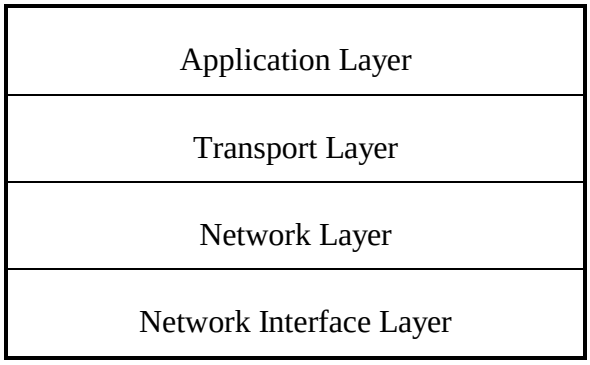


Figure 8. Internet Protocol Suite[††]

Reference to the IPS here is not intended to mandate its use, but rather to provide a framework for structuring functionality of the PMCS Internetworking Functional Entity. Additionally, OSI protocols have not achieved widespread acceptance; neither are OSI commercial item products readily available. The OSI RM is included here only to provide an additional structuring framework for PMCS internetworking functionality.

[††] The layered protocol architectures discussed here should not be interpreted as constraining the PMCS software architecture.

As previously discussed, the government explicitly recognizes that many existing types of RF network and some types of host networks may not be conducive to use within a layered model. Thus, support of certain legacy and migration systems may require functionality in other entities than Internetworking (specifically, Black-Side Functional Entities). It is anticipated that in the future, there would be a seamless network that is not specific to different types communications media. In fact, work already is being undertaken in this area.

A base level functionality suggested for PMCS is a rough equivalent to internetworking protocol architectures relying on connectionless service. However, due to military interests in ATM technology for both wired and wireless contexts, industry is invited to include ATM-based solutions, either separate from or in combination with internetworking architectures. The ATM protocol stack is depicted in Figure 9. The government recognizes that both native mode ATM application data as well as other protocols (for example, IPS) may be carried over this stack.

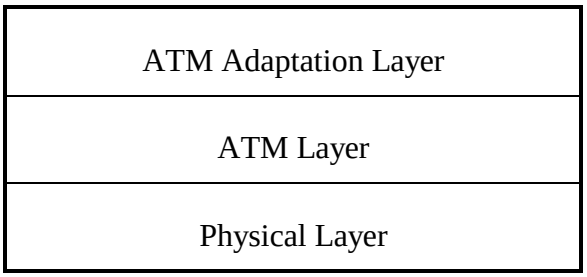


Figure 9. ATM Protocol Layers[††]

Some of the issues that are being addressed are highlighted below.

Connectionless Communications

Practice has shown that the connectionless approach facilitates scalability and robustness. Connectionless communications and loose coupling have been a major factor in the widespread success and acceptance of internetworking. Therefore, we suggest that the PMCS, as part of the Internetworking Functional Entity embody connectionless and loosely coupled, modular functionality based on accepted standards.

However, the government recognizes that due to stringent requirements of some current military and emerging civil aviation communications, as well as the need to continue use of legacy systems, some connection-oriented services and circuit switched services may be

[††] The layered protocol architectures discussed here should not be interpreted as constraining the PMCS software architecture.

needed. Discussion with industry will determine the extent to which the use of connection-oriented and circuit-switched service must be integrated to support the these needs.

Integrated Services Support

The PMCS should support both traditional, best-effort delivery as well as the real-time types of delivery required for emerging tactical communications applications and multimedia requirements. Though real-time, quality of service-based support historically has been absent from internetworking standards, architectures for integrated services are being developed by the networking community. Related protocols for functions such as resource reservation currently are being discussed as well.

However, it should be noted that this development is in its early stages and currently focuses on wired networks. Significant advancements in industry standards must occur before support for integrated services in wireless networks becomes a reality. Thus, provisions for integrated services support in PMCS are not necessarily expected in near-term proposals.

In longer-term solutions, support of integrated services should be provided for both wired and RF link types.

Where applicable, hybrid solutions involving internetworking and ATM should attempt to utilize the traffic management capabilities of ATM in enabling integrated services functionality within an internetworking architecture.

Security

Provisions enabling confidentiality, integrity, and availability may be needed in the network layer (and possibly other layers). The users' data should be protected from exploitation may be handled by INFOSEC. Security functionality will be provided by other Functional Entities beyond Internetworking (specifically, the INFOSEC Functional Entity).

Mobility Awareness

As in the case of integrated services, mobility awareness is an area of very active work in both the research community and standards bodies. The current focus of commercial interest is mobility of end systems and contexts in which the network infrastructure otherwise is fixed. Such a focus partially addressed government needs. However, the broader approach reflected in current work in mobile ad hoc networks and nomadic computing may be necessary to satisfy government needs completely.

Two significant aspects requiring investigation are protocols that efficiently use the constrained bandwidths expected in government networks, and provisions of protocols enabling rapid deployability and automatic configuration of non-fixed network infrastructure.

In longer-term solutions, awareness of mobility (of routers and hosts) will be necessary in at least the network layer, and possibly other layers as well. The impact of mobility on the basic data transmission service as well as on integrated services should be addressed.

Goals for Additional Functionality

- Ability to operate as an extension of existing communication networks.
- Technological, protocol, service, and application evolution through reliance on open system approaches.
- Support of use on a wide range of potentially mobile stations including those on board planes, ships, ground vehicles, and portable (possibly hand-held) devices.
- Minimal use of configuration parameters

Layered Functionality

In accordance with the layered model, it is expected that functionality be apportioned to the appropriate layer.

At least two emerging voice/data link systems are defining their internetworking architectures using layered functionalities: 1. NATO Improved Link Eleven (NILE), and 2. VHF Digital Link TDMA Mode (Mode 3). Industry attention is called to these systems only to provide examples of the scope of RF and host networking functions that might be supported. The following discussion provides further insight.

Application Layer Functionality

Any of the well-known application-layer protocols in the Internet correspond to commonly-used functionality in this layer, for example, file transfer, remote login, network management, and hypertext transfer.

Additionally, an application programming interface (API) to the services of the transport layer should be provided so that new, (possibly) military-specific, application-layer protocols can be developed and implemented. Normally, an application-layer protocol will access network functionality through use of the aforementioned API. However, it should be

possible as well for the application layer to access services of the network and link layers directly.

Presentation Layer Functionality

- Specification or negotiation of ways in which information is represented for exchanged by the application layer.

This layer often is considered to be null, in which case its functions are included in the application layer.

Session Layer Functionality

- Organization and synchronization of conversations over transport layer connections (when connections are used).

This layer often is considered to be null, in which case its functions are included in the application layer and transport layer.

Transport Layer Functionality

The transport layer is responsible for transferring data on an end-to-end basis (normally between hosts). The following basic functionality should be provided:

- Non-guaranteed datagram service
- Guaranteed, sequenced service with flow control and congestion control
- Data integrity
- Integrated services support

Network Layer Functionality

The network layer is responsible for enabling the interconnection of multiple networking technologies and transfer of data through the resulting *internetwork* in a consistent way that is independent of the specific technologies.

The following minimal functionality should be provided in this layer:

- Routing (intradomain and interdomain) in a way that attempts to minimize path cost
- Packet forwarding along selected routes

- Error reporting
- Fragmentation and reassembly
- Translation between link layer addresses and network-layer addresses
- Support for both multicast and integrated services
- Automatic configuration and adaptation to the maximum extent possible

Network Interface Layer Functionality (OSI: Link Layer plus Physical Layer Functionality)

The link layer is responsible for reliable transmission of information across the physical layer, sending blocks of data (frames) to the physical layer with the necessary synchronization, error control, flow control, media access control, data link services, and link management. Additional support for RF based networks is desired in the form of intranetworking functions, such as lower level connections (similar to LAP-B), non-user involved acknowledgments, and RF network topology information. Note that from the perspective of internetworking, certain of the link-layer functionality and network-layer is provided by other entities with which Internetworking interfaces.

There are current efforts and experimental implementations underway in this area, both in the government and private sector, and these efforts should be leveraged as much as possible for use in the PMCS.

The following functionality should be provided in this layer:

- For each link type, a method of encapsulating network-layer packets with link-layer frames should be specified
- RF network setup and reconfiguration (static and dynamic) specific to the protocol
- Methods for PMCS units to join/leave RF and other networks
- Any link layer functionality required to support upper layer, standards-based networking (for example, ATM link-layer functions, both wired and wireless)
- Media access control
  - Multiple access control and timing
  - Channel occupancy and congestion monitoring
  - System data and header formatting

  - Channel sensing
  - Automated handoff

- Data link services
  - Frame sequencing
  - Error detection
  - Station identification and addressing
  - Retransmission and acknowledgment

- Link management services
  - Link establishment
  - Link release
  - Link handoff
  - Link recovery
  - Link modification

B.5.6 Issues for Industry to Address

There are several Internetworking Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

- Near-term and far-term solutions, including transition plan(s)

- Networking requirements for new and emerging narrowband and wideband waveforms are either unknown or currently are being defined.

- Incorporation of Tactical Internet functions with growth for the future

- Network protocol standards (and changes to support military requirements)

- Mobility awareness

- Integrated service/QoS support

- Support of network management functionality

- Appropriateness of commercial hardware and software

- Security

- Ruggedization
- Network management
- Configuration and reconfiguration of internetworking parameters
- Integrated training

B.6 SYSTEM CONTROL FUNCTIONAL ENTITY

B.6.1 Functional Definition

Within the PMCS SRM, the System Control Functional Entity is intended to provide overall internal system control. This includes control of the system state (e.g. initialization, operational, shutdown, maintenance), control of all other Functional Entities, and control of Built-In Test (BIT) capabilities. The System Control Functional Entity is the mechanism by which all system adjustments and reconfigurations are made. Also, it must have the ability to perform all tasks in a deterministic fashion and satisfy specific timing requirements within PMCS.

It interacts with all other entities, as shown in Figure 10, by sending and receiving control information such as commands, status, and parameters. The interfaces shown in the figure are notional and convey the peer-to-peer exchange of control information between entities.

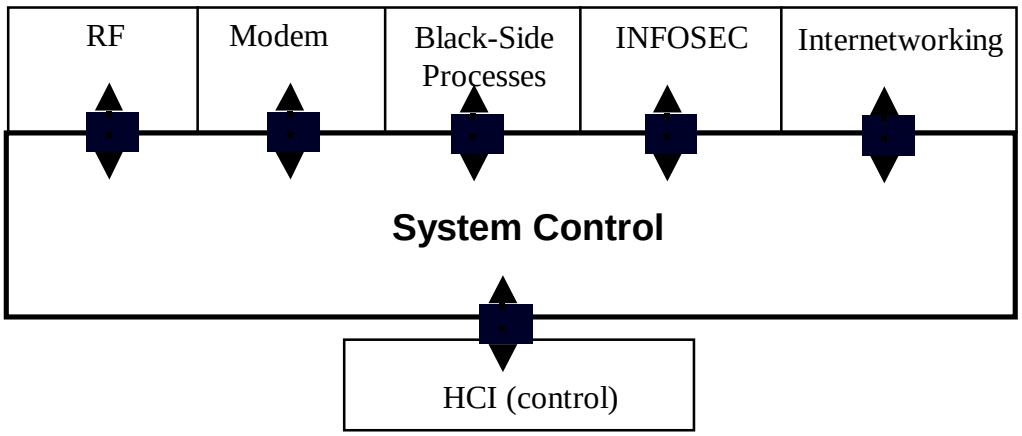


Figure 10. System Control logical interfaces with other PMCS Functional Entities

Note: Although System Control may initiate the use of a specific waveform application, it is not intended to be directly involved in specific waveform processing, data processing, or network processing operations. Unique control functions required for these specific operations should be implemented within the appropriate Functional Entity.

The System Control Functional Entity manages the different states of the PMCS and controls the resources needed to execute the states. This includes

- Loading new software

- Start-up/shut-down
- Instantiation of a virtual radio channel (RF to I/O), re-instantiation
- Changing virtual radio channel parameters
- Changing to a different virtual radio
- Monitoring status during normal operation

System Control connects to the user through HCI. It receives system commands and parameters input from HCI, and sends system status output to HCI.

System Control also works with INFOSEC to support the PMCS security monitor function. System Control must provide appropriate security access functions to use and modify system and application software programs.

Management of Smart Radio functions may also reside in System Control. This includes over-the-air reconfiguration, assessing channel availability and utilization, and graceful degradation.

B.6.2 Critical Sub-functions

System Configuration: System Control should be able to configure the PMCS via simple commands to the other entities. This would require the individual entities to intelligently process the System Control commands to configure down to the smallest adjustable units within each Functional Entity. The configuration of the system can be directed either through the HCI Functional Entity (via direct connection, over the Host networks, or over the RF networks) by a user, or through the automatic reconfiguration capability described below.

- System Configuration Presets:

To accelerate reconfiguration, the System Control Functional Entity may maintain a set of configuration settings. These settings would be activated by a single command from the HCI Functional Entity to activate and reconfigure one or more of the virtual radio channels. This functionality may facilitate automating the insertion of a communications plan in each individual PMCS by a user.

- Automatic Reconfiguration:

It may also be possible for the PMCS to reconfigure itself when a particular channel is determined to be unusable. Through its BIT and operations execution capabilities, the PMCS could have the ability to automatically reconfigure its radio assets to recover a communications channel lost due to RF interference, line of sight blockage, equipment damage, or other difficulty.

- Automatic Software Validation:

As a goal, System Control would perform validation checks as part of initiation to help determine the compatibility of the software loaded onto the individual Functional Entities.

Built-In Test (BIT): The System Control Functional Entity commands the other entities to perform BIT, collects the responses from the entities, and reports the BIT information to the HCI. BIT functions may be performed on demand and at regular intervals in the background of other PMCS functions.

Operations Execution: The System Control Functional Entity ensures that other Functional Entity resources are assigned for proper execution of user-desired PMCS operations. Once operations are established, System Control queries the other entities and reports their system performance. This may be possible for some waveforms and not for others. When possible and desired by the user, this may include, but not be limited to, the following:

1. *Radio link performance:* Bit error rates, signal-to-noise ratio, fading characteristics, interference environment measurements, etc.

2. *Networking performance:* Data transmission rates, dropped packet statistics, connection statistics, etc.

3. *Encryption system performance:* Synchronization statistics, suspected attempts to attack the communications network through illegal entry, etc.

Database Management: System Control must manage the PMCS internal database for storing, updating, and sharing system information that is needed for PMCS to operate properly. This includes the collection and dissemination of information such that other PMCS entities may make proper decisions and take appropriate actions.

B.6.3 Critical Interfaces

System Control interfaces with each of the other entities within the PMCS to coordinate and manage the system states. However, every application of PMCS may not have all the entities

or may have different versions of the entities. It is expected that the System Control intercommunication and management mechanism would have the flexibility to provide for this configurability, scaleability, and extendibility. This is a key reason why System Control is designated a Functional Entity with logical interfaces to the other entities. The mechanism used to coordinate and to intercommunicate with the other Functional Entities has yet to be defined. One possible concept is to have PMCS Functional Entities register with System Control. The System Control Functional Entity could then recognize the installed PMCS configuration and establish the appropriate control, BIT, and monitoring activities.

HCI Functional Entity Interface: System Control shall provide complete access from all of its capabilities to the HCI Functional Entity. It shall also provide system test and system performance information to the HCI Functional Entity. This information shall include, but not be limited to, warning messages and system interrupts in the case of equipment failure detected by the System Control Functional Entity.

Internetworking Functional Entity Interface: Since many networking protocols strongly couple the control of the various protocol layers, it is incumbent upon the System Control Functional Entity to provide an interface to the Internetworking Functional Entity. This interface should provide access to the system configuration preset capabilities. The System Control Functional Entity should also be able to provide the HCI Functional Entity with warning or system interrupt messages when the Internetworking Functional Entity initiates changes to the system configuration.

INFOSEC Functional Entity Interface: The System Control Functional Entity shall interface with the INFOSEC Functional Entity to perform security monitor, application load, and BIT functions.

Black-Side Processes, Modem and RF Functional Entities Interface: The System Control Functional Entity shall have access to as many of the adjustable parameters within these entities as is necessary for controlling system configurations. System Control may have a "Black-side" element to interface with the Black-Side Processes, Modem and RF Functional Entities. This Black-side control would reduce the amount of control information that crosses the red/black boundary. The System Control Functional Entity shall also be able to trigger or perform BIT functions on both of these entities over this interface.

B.6.4 Issues for Industry to Address

There are several System Control Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

- Intercommunication architecture and protocols between System Control and the other Functional Entities
- Functional partitioning and definition of critical sub-functions, including concept for black and red-side partitioning
- Central versus distributed control (external and internal to PMCS)
- Control authentication/certification concept for user access
- Database management options (i.e., Management Information Base)
- Performance monitoring options and cost

B.7 HUMAN-COMPUTER INTERFACE FUNCTIONAL ENTITY

The Human-Computer Interface (HCI) Functional Entity describes the functions necessary for the user to interact with PMCS. The guidance in this section applies the information from the JTA to PMCS, and is not intended to contradict nor supersede the JTA. The JTA provides a common framework for HCI design and implementation options in DoD systems. Chapter Five of the JTA document specifies HCI design guidance, mandates, and standards. For the PMCS, HCI development should follow the mandates and recommendations found in the JTA appropriate to mission, platform and user requirements.

Note: The "human" aspect in the definition of this Functional Entity should be considered functional, rather than physical. The name does not imply that a human must always interface with PMCS. The interface to the HCI could be human, or the input/output functions could be automated by machine.

B.7.1 Functional Definition

HCI includes the overall performance of the system with the operator in the loop, and the appearance and behavior of the interface, physical interactions devices, graphical interaction objects, and other human-computer interaction methods. It should be both easy to use and appropriate to the operational environment. Operational environment considerations, such as military threat for example, should be considered. Subsets of HCI include the functional allocation between the user and the system based on operational requirements, number of users, human capabilities and limitations, and the anticipated difficulty of mission phases and tasks. HCI includes the interface characteristics (system features, display formatting, information coding, etc.). as well as interaction methods (visual, auditory, tactile, etc.). The HCI Functional Entity exhibits a combination of user-oriented characteristics to support:

- Intuitive operation aligned with human cognitive capability
- Ease and retention of learning including embedded crew training and operational simulation
- Facilitation of user task performance and situational awareness
- Consistency with user expectations
- Customization for specific needs

- Emulation or adaptation of existing legacy interfaces to the extent practicable, incorporating accepted HCI design concepts (Avoid perpetuating existing poor HCI designs)

- Considerations for information warfare including real time and near-real time data collection, correlation, fusion, and information distribution

- Incorporation of decision aiding and adaptive automation techniques

- Adequate feedback to the users

- Environmental stressor considerations for user and system safety and health (temperature, humidity, lighting, vibration, etc.)

Sub-Functions

HCI can be difficult to quantify because the extent of functionality in this Functional Entity is greatly affected by specific missions and platforms. Each HCI will have a "personality" or tailoring unique to the platform or mission. However, two basic aspects of HCI may characterize the functionality: the location of the HCI, and the type of information processed by the HCI. Figure 11 represents the general characterization of HCI functionality to account for the two HCI aspects of location and information. The specific HCI implementation may only include a subset of the four major blocks shown in the figure. Also, note that security concerns for information warfare should be considered for all aspects of HCI. Security for HCI may be shared across the INFOSEC and Internetworking Functional Entities. Refer to the JTA for more specific guidance that addresses HCI security.

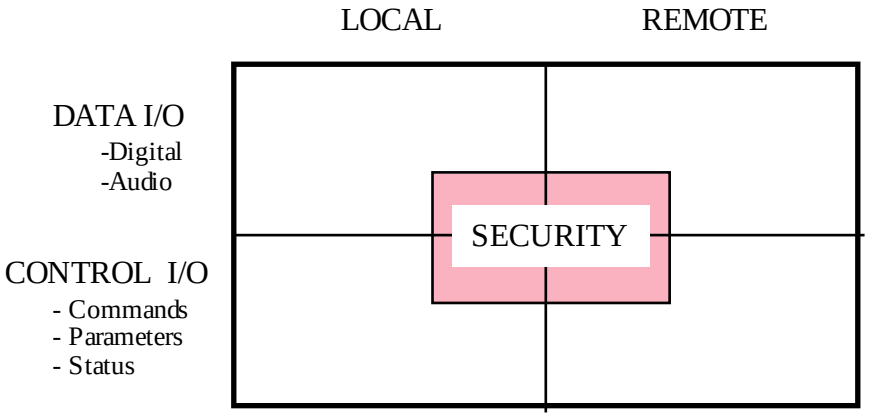


Figure 11. General Characterization of HCI Functionality

HCI Location

The *location* of HCI functionality could be remote and/or local. "Local" is interpreted here to be physically part of, attached to, or directly connected to, a PMCS chassis such that the HCI distance from the PMCS chassis is measured in inches. "Remote" is interpreted here to be a unique functional implementation separated by some measured distance from the main PMCS chassis. The term "remote" applies to connection of the HCI to PMCS via platform LANs and busses, or wider connection crossing longer distances. For example, baseband connection over telephone lines, microwave, WANs, and tactical data link connections. The partitioning of sub-functions to local or remote HCI implementations affects the specification of the data transport mechanisms, and the interface boundaries of HCI. An example implementation could be placement of the HCI in an airport tower, placement of the RF and modem in a hangar, and placement of the antenna in a nearby antenna field. Location will impact design relative to the physical environment of the system (lighting intensity, temperature, humidity, vibration, electromagnetic interference, etc.).

HCI Information

The type of information processed by HCI is considered either Data or Control. Data is further subdivided as digital or audio (analog). In general, data inputs to PMCS would be connected first to HCI to be processed, digitized (for audio), and formatted (if not already formatted). Some formatting may be application specific.

Control information is either a command, status, or parameter. Commands affect the selection of specific functions in the other PMCS entities. Parameters uniquely specify the configuration of a PMCS application. Status indicates the operation and readiness of PMCS, and includes BIT, error messages, and alarms.

B.7.2 Critical Sub-Functions

The following are considered the critical sub-functions of HCI:

User control: HCI would be used to set up and control the PMCS. The entry and display devices for this control information may be platform specific but the type of information, functions, and processing should be standardized. The HCI will assemble the control information into a standard format for input to the System Control Functional Entity. The standard format will include the commands and parameters from HCI into PMCS, and the PMCS status reported to HCI.

The HCI must provide for temporary storage of control information prior to loading into the PMCS database. The HCI must also provide for a means of loading new software into PMCS.

User data I/O: The HCI presents a data interface that adapts to the user on one side of HCI, and to the PMCS Internetworking Functional Entity on the other side of HCI. HCI performs the necessary conversion of the audio, and formats digital data for input/output with the Internetworking Functional Entity. HCI may also include audio drivers, line amplifiers, and signal conditioners necessary for sending the audio to speakers, headsets, or line connections.

Display: The HCI must have the means to display status information to the user. Also, HCI may be used to display user data sent over PMCS links.

Security: HCI must have appropriate access control to support provisions for various levels of access to PMCS capability. HCI must also support entry of information for INFOSEC devices.

B.7.3 Critical Interfaces

HCI should use an open standard I/O messaging scheme to pass information to and from the System Control and Internetworking Functional Entities of PMCS. The interface from HCI to the display should also be an open standard interface.

B.7.4 Legacy Issues

Adapting PMCS to meet the needs of many legacy systems will be a challenge. However, the functions of HCI should be standardized, with the unique tailoring most evident in platform-specific implementations. Tailoring to meet legacy system requirements should not lead to PMCS HCI design inadequacies.

B.7.5 Issues For Industry To Address

There are several Human-Computer Interface Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

- Defining a family of configurations that leverages technology to satisfy diverse mission and environmental constraints

HCI does not have one size that fits all. The HCI sub-functions must be defined sufficiently to allow them to be combined as needed to satisfy diverse mission requirements and legacy system uniqueness.

- Maintaining Open Systems architecture (standards based interfaces) across multiple systems, platforms, and applications.

  Commonality across PMCS implementations may be difficult to achieve. The JTA guidance will be helpful in this area.

- Minimizing integration of capabilities for legacy systems.

  Legacy systems have unique and often inadequate HCI capability. Interfacing to these legacy systems with minimal impact poses many technical challenges.

B.8 CRITICAL SYSTEM INTERCONNECT FUNCTIONAL ENTITY

B.8.1 Functional Definition

The Critical System Interconnect (CSI) is the infrastructure (underlying framework) of the PMCS. All the previously discussed Functional Entities are implemented in hardware and software modules and interconnect and integration is key to PMCS. CSI defines the mechanical format of the hardware modules, the electrical definition of the hardware modules' backplane bus interface and the type of protocol used to communicate between all modules. The Critical System Interconnect also implements any special internal interfaces beyond the backplane bus. It also defines the mechanical and electrical requirements of the chassis or enclosure. The three way or external interfaces (RF, Internetworking, and HCI) are also included in CSI.

The chassis nomenclature is typical of military radio configurations but alternatives may exist that can satisfy both the commercial marketplace (e.g., general aviation) and the DoD and FAA operational environments.

The data buses illustrated in the Electrical, Control Interconnect part of the table indicate data buses which may be used for passing data, control, status information throughout PMCS on both the red- and black-sides, and may be used for appropriate external interfaces as well.

The sub-module interconnect data buses are for illustration only and indicate the potential need for special data buses either internal to Functional Entities or between Functional Entities (e.g., RF to Modem).

B.8.2 Standards

The criteria for selecting the model interconnect is an open system approach. (See A.5). An open system approach achieves a scheme in CSI performance capability as an affordable solution. The JTA is the starting point from which to select PMCS standard interfaces. If the JTA does not have a particular standard identified, standards are selected that meet the criteria for: 1. PMCS performance, which includes size, weight, and power (SWAP); 2. environmental constraints; and 3. being widely used and accepted standard interface.

Table 2 lists configurations and open system standards that may be candidates for PMCS.

Table 2. Candidate Open System Standards

Standards	Fixed Station	Airborne	Personal	Maritime	Ground Mobile
Chassis					
19” Rack Mount	X	X		X	X
ATR Chassis		X			X
Manpack			X		
Desktop	X			X	
Module Mechanical					
IEEE 1101.10 Convection cooled 6U x 160mm and 3U x 160 mm	X	X	X	X	X
IEEE 1101.2 Conduction cooled 6U x 160mm		X		X	X
IEEE 1101.4 Conduction cooled SEM E		X			X
PCMCIA Type III	X		X		
EISA/ISA	X		X		
ANSI/VITA-20 VME FOR SEM E		X			X
Electrical, Control, Interconnect					
ANSI/VITA-1	X	X		X	X
IEEE 1394 and extensions	X	X	X	X	
PCI	X		X	X	X
EISA/ISA	X				
Sub Module Interconnect					
ANSI/VITA-2 Raceway	X	X	X	X	X
IEEE 1386.1 PMC	X	X	X	X	X
ANSI/VITA-18 CCPMC	X	X	X	X	X
ANSI/VITA-4 Industry Pack	X	X	X	X	X
IEEE 1096 VSB	X	X	X	X	X
Ethernet					
10 Base2	X			X	X
10 BaseT	X			X	
100 BaseT	X				

B.8.3 Domain (Operational Environment)

The government recognizes that there are many different environments for which a PMCS is applicable. Typical domain environments have been identified, as Personal (e.g., Dismounted Soldier, etc.), Maritime, Airborne, Ground Mobile, Fixed Station (see Figure 12). The selection of one common mechanical and electrical interconnect scheme may not be optimal for every environment. However, the government seeks a common solution, as much as possible, that will be cost-effective and not compromise the effectiveness of the user.

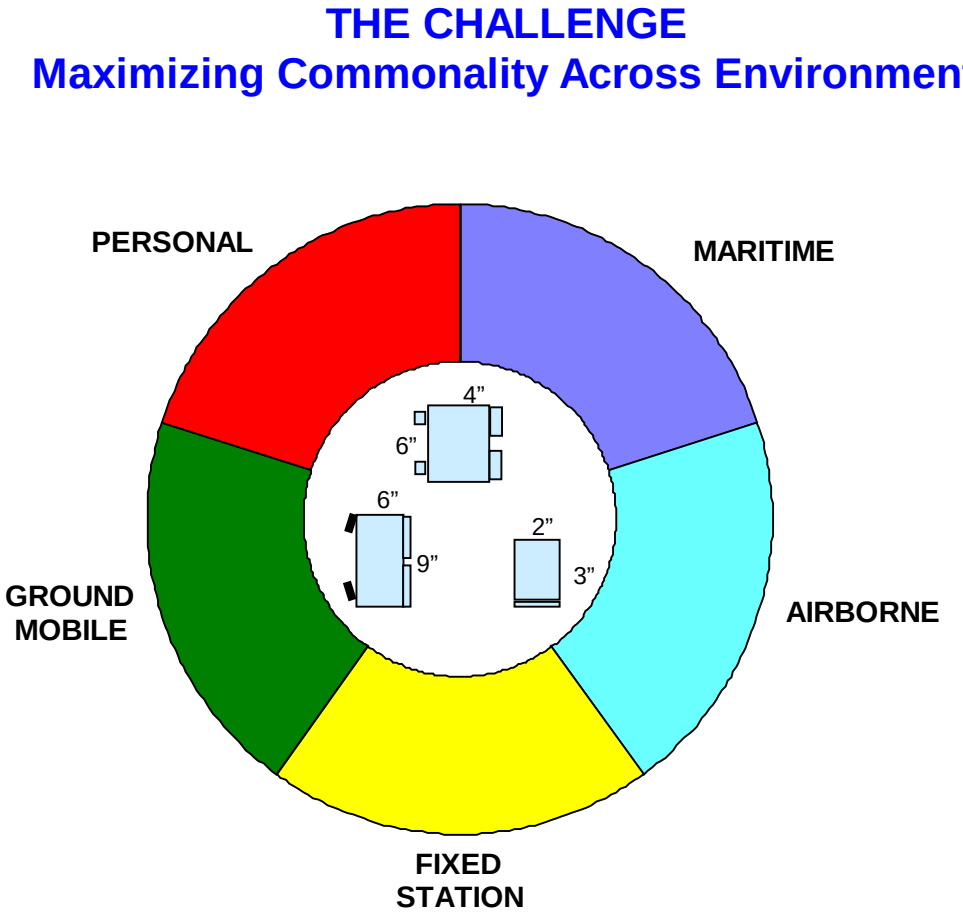


Figure 12. Domains

B.8.4 Chassis

The radio market for the government has two major categories: new acquisition and retrofit of existing platforms. The chassis chosen will fit into platforms and will allow for insertion of the module standards selected. All standards and specifications incorporate open systems standard interfaces. This then provides common module specifications for all radio acquisition programs.

B.8.5 Module

The term module relates to implementations of both hardware and software. Hardware modules are discussed here and software modules are discussed in Section C.

The hardware modules that implement each Functional Entity should be based on widely used and accepted industry standards. They address the needs of SWAP, and environmental requirements of current and future platforms.

Modules will communicate over a common backplane bus standard. This common backplane bus standard will pass status, control, timing, and power to all the hardware modules. It may pass data. This will be considered a common hardware module interface. The modules may need to communicate message, status, and control information between Functional Entities. This interconnect will be referred to as a specific functional module interface. Both common and specific module interfaces should be widely used and accepted standard interfaces. The functional module interface should not be proprietary.

There are a few Functional Entities, (e.g. RF and Modem), that could require special synchronous timing. This timing could be distributed to these and other Functional Entities over the common backplane bus or through the specific functional module interconnect. This timing interconnect should be a widely used and accepted standard interface.

B.8.6 Issues for Industry to Address

There are several Critical System Interconnect Functional Entity issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SRM. These are as follows:

What standard timing references would be used to provide a standard method for distributing a synchronous timing reference signal? Would timing signals such as IRIG-B be adequate?

What materials should we be using to:

- Reduce size and weight
- Provide protection from EMP and EMI/EMC

What techniques should PMCS be using to provide EMI/EMC protection between the PMCS Functional Entities and between the PMCS and external system?

Power Supplies—How to integrate and standardize a common power supply and distribution system for personal, ground mobile, maritime, avionics PMCS solution.

Module interfaces to the common backplane bus must be based on widely used and accepted standards.

Entities could be combined in a specific application's system implementation if life cycle studies and industry trade studies show a significant savings and performance increase.

Design and integration of entities must address system-wide Security and EMI.

Fail Safe Power—How to integrate uninterruptable power supply (UPS) capability for each PMCS Domain.

Battery Life Management—How do we incorporate smart battery management to extend battery life?

C. SOFTWARE REFERENCE MODEL

C.1 SCOPE

The Software Reference Model (SwRM) addresses the software within each of the Functional Entities of the System Reference Model and the software-related relationships between these Entities. Software is addressed separately in this section since it is envisioned to be a major component of the PMCS. Software will be a critical factor in achieving the broad set of DoD and FAA requirements and the ability to change and upgrade the PMCS. The "openness" of the software architecture and design is key to leveraging an envisioned vendor base skilled in radio communications products.

The SwRM is composed of two views: a Notional view and a Layered view. The Notional view addresses the software for each of the Functional Entities and shows their software inter-relationships, i.e., a notional concept for how they fit together and interact. The Layered view addresses the layered design required for all the software applications and services, and between software and hardware for all of the Functional Entities.

C.1.1 Terms and Definitions

The following section provides definitions for some of the terms that are used throughout this Section C.

Functional Entity: Any of the major functional components identified in the PMCS System Reference Model.

Software Entity: A bounded software application, software service, or operating system with a well-defined function and open interface.

Software Application: Software that meets a particular user requirement.

Software Service: Software that provides services that are common across multiple applications.

Operating System: Software, including device drivers, that provides an interface to the hardware.

Hardware: For this section, hardware refers to the physical entities on which the software executes and the physical entities used to communicate with other software, i.e., bus interconnects, network interconnects, etc.

Application Program Interface: A defined interface that allows a software application to transparently access lower-level services (including the operating system and hardware).

C.1.2 Objective

The objective of the SwRM is to provide a framework, which supports:

- Programmability to meet mission requirements
- Modularity to allow software reconfiguration and reuse
- Multi-sourcing of portable, scalable, extensible software
- Upgradeability or migration to new software/hardware technology

This SwRM does **NOT** dictate a specific physical configuration or partitioning. The main purpose is to help explain the open modular concept as it applies to communication systems. Openness and modularity of a PMCS are achieved mostly in software modules rather than hardware components. The SwRM is designed to facilitate software and hardware development and upgrades with reduced cost and system impact. Therefore, PMCS software must be:

- Modular in the sense of accommodating different hardware configurations
- Scalable in the sense of accommodating Quantitative Growth (i.e., duplication of modules to accommodate multiple channels)
- Extensible in the sense of accommodating Qualitative Growth (i.e., increased functionality such as additional waveforms, networks, interfaces)
- Portable in the sense of providing independence with respect to hardware implementations, interconnects, and operating systems.
- Trusted in the sense of being designed using NSA-SEI's Trusted Capability Maturity Model

- Reusable in the sense of providing and maintaining libraries of waveforms, functions and primitives

- Open in the sense of using commercial languages, interfaces and tools

C.2 SOFTWARE REFERENCE MODEL: NOTIONAL VIEW

Figure 13 shows the notional view. This can be thought of as the "floor plan" or top view of the SwRM. The notional view shows the software interfaces between Functional Entities. It relates the SwRM to the Entity Reference Model by identifying the critical interfaces of the Software Entity encompassed within the Functional Entity. Rather than representing physical or direct interfaces, these critical interfaces identify the logical information flows between and among Functional Entities. The critical interfaces are logical peer-to-peer interfaces (similar to the SAE Generic Open Architecture). Once standardized, these open interfaces define interoperability requirements and foster independent development of Functional Entities. A key task for the PMCS community is the standardization of these interfaces.

The notional view shows how these Software Entities are "notionally" or logically connected for data flow through PMCS, and control flow within PMCS. In Figure 12, the critical interfaces are separated into control and data interfaces and shown orthogonally. "Data" is generally interpreted as the user information that flows through the system. "Control" is interpreted here as system commands, parameters, and status used within and for PMCS.

The key attributes of this view of the SwRM are:

- *Software Entities*—sufficiently well-defined to foster commercial development at the entity level.

- *Embedded Security*—a critical aspect of the model that affects both the data and control flow.

- *System Control*—routing all system control information through one entity supports security, consolidates state information, and simplifies the control interfaces of the other software entities.

- *De-coupled HCI*—standardized HCI-System Control interface allows multiple choices for HCI implementation and supports "personalization" for either or both the user control and host data interfaces.

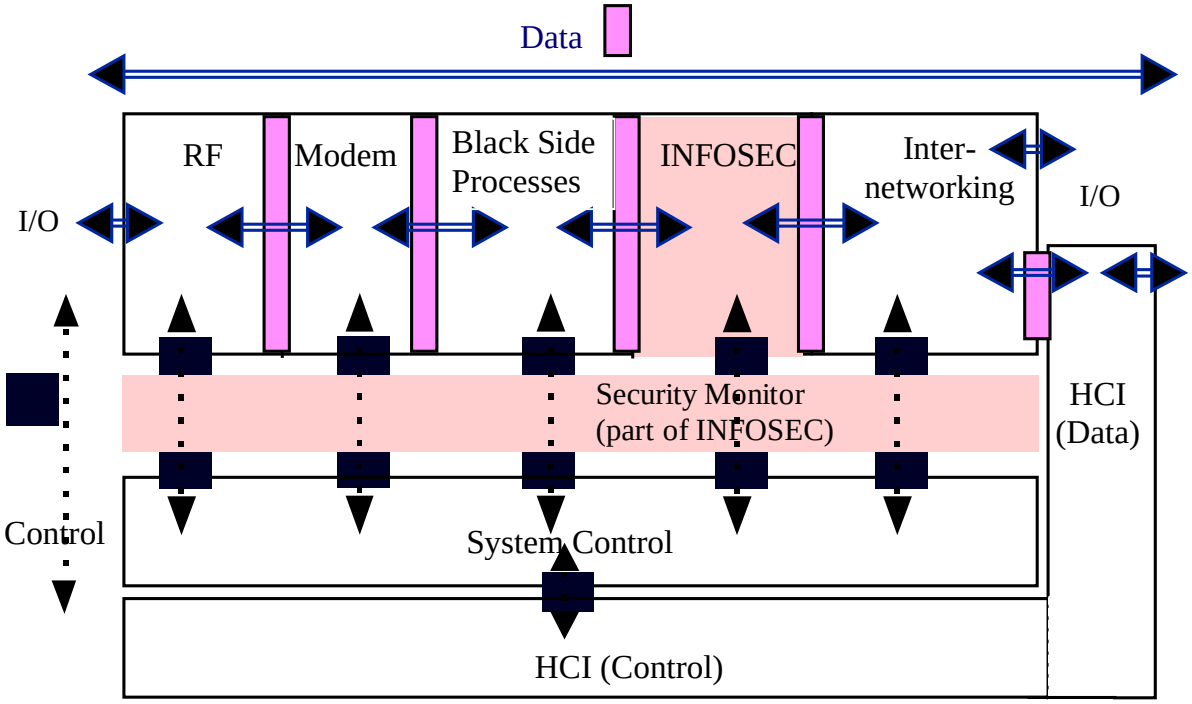


Figure 13. Notional View

C.2.1 Software Entities

The identification of system interfaces and sub-functions defines the PMCS Functional Entities at a notional level; specification of standard interfaces for Software Entities formalizes the boundaries of Functional Entities and creates a truly open PMCS. The Software Entities are identified with the same names as the Functional Entities defined in the PMCS ERM. However, there are significant differences. A Software Entity may or may not have a one-to-one mapping to the underlying hardware of the Functional Entity. For example, multiple Software Entities may reside (and be multi-tasked) on the same hardware, as long as the critical interfaces are maintained.

C.2.1.1 Embedded Security

Embedded security is highlighted in Figure 13 to show that it is an integral part of both the data flow and control flow in PMCS. The Security Monitor assures that the System Control information is not misdirected. It is shown here as a part of INFOSEC because it affects the internal security of PMCS, and it is considered a critical software sub-function.

C.2.1.2 System Control

The wide box is drawn for System Control because it manages the total system state and provides a single functional interface for the user from the HCI to the other Functional Entities. Because of its importance, System Control is considered a critical software function. As shown here, it affects both the "Black-side" and the "Red-side" entities. The Software Entity for System Control will always have a primary or master component on the "Red-side" of a PMCS implementation with embedded security. However, there may be a secondary or slave component of System Control software that resides on the "Black-side." This partitioning of System Control should be transparent to the other Functional Entities.

System control is difficult to implement in a system of distributed processing elements. Standardizing the partitioning of control functions between the different Functional Entities and the System Control Functional Entity is another important task for the PMCS community.

C.2.1.3 De-coupled HCI

The PMCS SwRM isolates the HCI to a single interface with System Control. This provides maximum flexibility, allowing the HCI to be implemented locally within PMCS or externally through a network. It is believed that special-purpose HCIs may be standardized (e.g., sets of diagnostic graphs) and run in conjunction with standard HCIs. The HCI should be adaptable to the mission and user needs.

Note that the HCI is shown wrapped around the other entities because it has both control and data functions. These functions must be separately identified within HCI so that they may be tailored, if necessary, to address platform and mission specific requirements. Both may have important legacy requirements which must be addressed.

C.2.2 Software Interfaces

The critical software interfaces of the Notional view can be grouped into three categories:

- Data Internal Interfaces
  - RF-Modem
  - Modem-INFOSEC
  - INFOSEC-Internetworking
  - Internetworking-HCI
  - HCI-Internetworking

- Control Interfaces
  - System Control to RF, Modem, INFOSEC, Internetworking, HCI

- Data External Interfaces
  - RF-external
  - Internetworking-external
  - HCI-external

It is important to understand that the entities in the ERM and SwRM are envisioned to change frequently and in an uncoupled manner, and that the critical interfaces will be updated as necessary to allow for growth and cost reduction.

C.2.2.1 Data Internal Interfaces.

The internal data interfaces describe the peer-to-peer data exchange between the Functional Entities of PMCS, including timing information required for specific waveform applications. Some of these interfaces may need to support high speed data exchange of time-critical information between entities.

C.2.2.2 Control Interfaces.

The Control Interfaces affect all the software entities, but are most affected by the System Control Functional Entity and the Security Monitor of the INFOSEC Functional Entity. The control interfaces define logical system control information exchanges between two entities without regard for the path (e.g., through INFOSEC) by which the information is exchanged. In defining these interfaces, careful consideration must be given to those control aspects that are generic inter-entity system functions, and the control aspects that are specific to a waveform application within a Functional Entity. System Control is not intended to be directly involved in controlling specific “waveform” applications. Unique control functions

required for a specific application should be implemented within the appropriate Functional Entity. Standardizing the control interfaces will involve decisions as to which side of the interface should control capabilities reside (i.e., how "smart" to make each of the Functional Entities). The control interface to HCI may be the most straightforward. Therefore, System Control should present a standard interface to HCI (e.g., Management Information Base (MIB)).

C.2.2.3 Data External Interfaces.

The three External Data Interfaces mark the boundaries where PMCS interfaces with humans and with external, often legacy, systems. Unlike the as yet undefined inter-entity interfaces, there are existing standards that provide good candidates for External Digital Interfaces to PMCS, such as Ethernet and TCP/IP for interfacing to the Internetworking Functional Entity..

C.3 SOFTWARE REFERENCE MODEL: LAYERED VIEW

Figure 14 shows the Layered view of the SwRM. This can be thought of as the "side view." The use of layering provides independence of the software applications from the underlying physical implementations. This is a key constraint. In the figure, the API is the Application Program Interface; the OS is the Operating System, or functional equivalent; and the EEI is the External Environment Interface that provides a direct connection to the Critical System Interconnect.

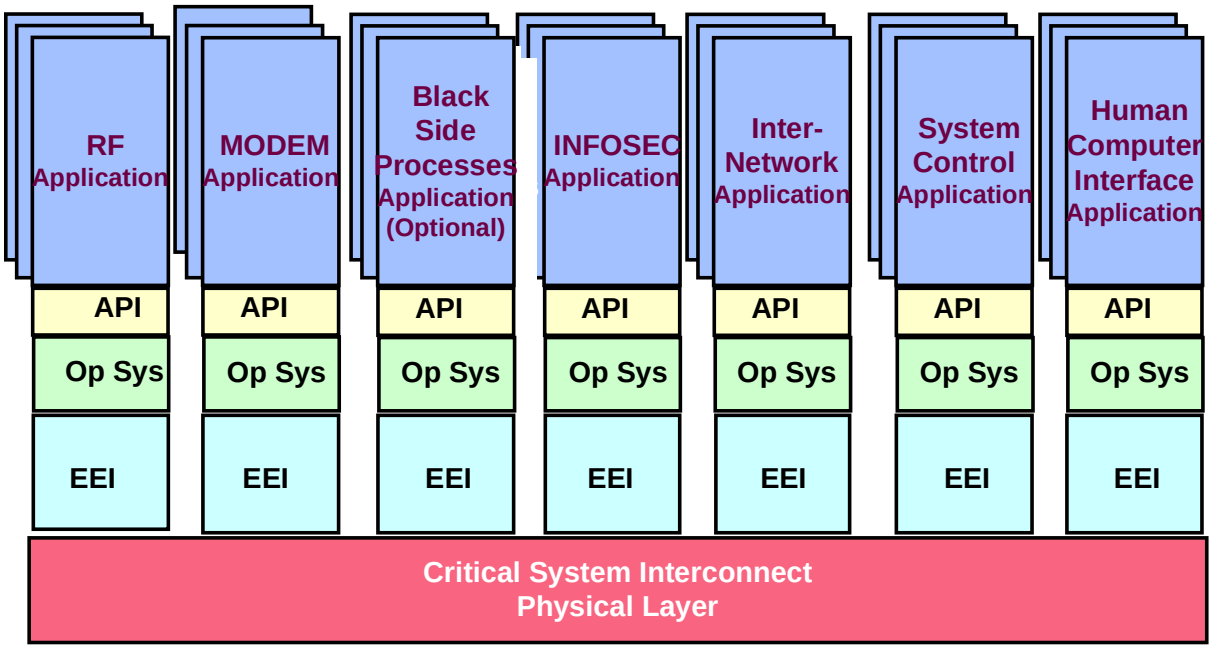


Figure 14. Layered View

Note: Upper layers may have one-to-one, one-to-many, or many-to-one relationships with lower layers (e.g., several applications may run on one operating system).

C.3.1 Key Attributes

The key attributes of the Layered view of the SwRM are to depict:

- Software independence from underlying hardware
- Software application independence from other software applications
- Common software services shared among multiple software applications

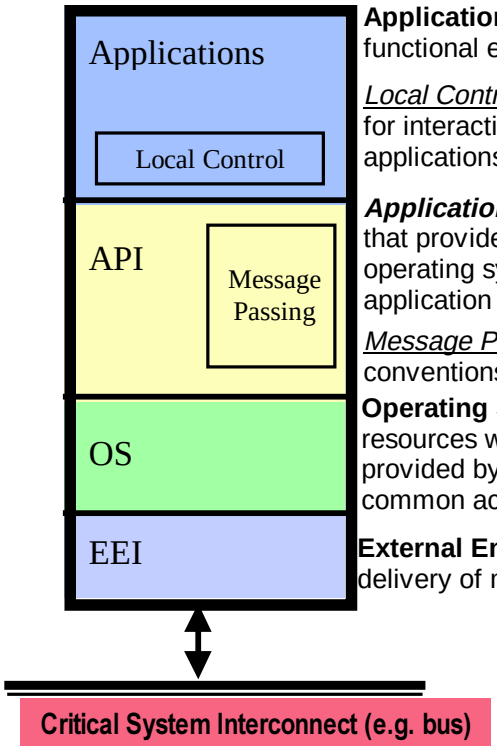
These attributes are achieved by standardizing the direct interfaces between layers. At the application interface, well-defined APIs provide the syntax and semantics of any message formats, procedure calls, or global data shared between entities. For example, POSIX defines an API between an application and an operating system. The POSIX API allows replacement of one POSIX-conformant operating system by any other POSIX-conformant operating system without affecting applications. Whereas POSIX is a recognized standard for general

purpose operating systems, no industry-wide standards currently exist for real-time operating systems. This is a major difficulty for some entities of the PMCS. PMCS may require the use of real-time operating systems for RF and Modem, while INFOSEC, Internetworking, System Control, and HCI may be able to satisfy performance requirements using general purpose operating systems.

C.3.2 Critical Software Interfaces Between Layers

Figure 15 depicts an expansion of the Layered view for a generic software entity. The critical software interfaces are the API and EEI. The API and EEI isolate the applications and the OS from the Critical System Interconnect.

This model does not imply that one common OS is to be used throughout PMCS. Proper definition of the API and EEI would permit different operating systems to be used for different entities.



Applications: These are the software programs specific to a functional entity.

Local Control: This subfunction provides a common control interface for interacting with System Control, and manages intra-entity applications.

Application Program Interface (API): This is a common set of calls that provides a level of abstraction between the application and the operating system or other services to ensure portability of the application code.

Message Passing: This critical subset of the API defines the calling conventions for intercommunication among entities.

Operating System (OS): This manages the processes, files, and resources within the functional entity. These OS functions could be provided by COTS, or "home- grown." The OS does not have to be common across entities.

External Environment Interface (EEI): This provides reliable delivery of messages between entities connected to the common

Figure 15. General Layered View Expanded

Figure 15 highlights Local Control within PMCS applications as a critical sub-function that defines the interaction with System Control and provides specific control within the entity.

The Message Passing layer is also highlighted as a critical subset of the API that standardizes data communications between software entities. Message Passing provides the inter-communication between Functional Entities to support scaleability and Functional Entity independence. The Local Control sub-function abstracts any control processing within a software entity and Message Passing abstracts all the details of packaging, parsing, and exchanging messages. Creating these sub-functions simplifies development of the entities and produces two strong candidates to be reused in other PMCS software entities.

C.4 SOFTWARE TECHNICAL ISSUES

There are several Software Reference Model issues for industry and government to address as the definition of a PMCS Systems Architecture evolves from the PMCS SwRM. These are as follows:

- Programmability and reconfigurability to meet mission requirements
  - Loading new software in the field or possibly during a mission for reconfiguration and/or recovery
  - How can this be done simply (e.g., as on a desktop computer)?

- Software reuse libraries
  - What software entities can be reused?
  - What is the right level of modularity?

- Message-passing implementation
  - What is the recommended approach?

- Degree of “Smart” Functional Entities
  - What local control capabilities should be in each Functional Entity?

These issues are stated simply and briefly, but they cover a broad area of topics including development, operation, and support.

APPENDIX A - ACRONYMS

A/D	Analog to digital
AGC	Automatic gain control
AM	Amplitude modulation
AM-SSB	Amplitude modulation single side band
ANSI	American National Standards Institute
API	Application program interface
ARITA	Airborne Reconnaissance Information Technical Architecture
ATE	Automatic Test Equipment
ATM	Asynchronous Transfer Mode
ATR	Air Transportable Rack
BIT	Built in test
C4	Command Control, Communications and Computers
C4I	Command Control, Communications, Computers and Intelligence
C4ISR ITF	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Integration Task Force
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCPMC	Conduction Cooled PMC
CD-ROM	Compact Disk Read Only Memory
COMSEC	Communications security
CPU	Central processing unit
CSI	Critical System Interconnect
D/A	Digital to analog
DoD	Department of Defense
DSP	Digital signal processor
EEI	External Environment Interface
EISA	Extended Industry Standard Architecture
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EPLRS VHSIC	Enhanced Position Location Reporting System Very High Speed Integrated Circuit
EMP	Electromagnetic pulse
ERM	Entity Reference Model
F3I	Form, fit, function, and interface
FAA	Federal Aviation Administration
FEI	Functional Entity Interface
FH	frequency hopped

FIPS	Federal Information Processing Standards
FM	frequency modulation
FPGA	field programmable gate arrays
FSK	frequency shift keyed
GHz	Giga Hertz
GPS	Global Positioning System
HCI	Human Computer Interface
HF	High frequency
HFAJ	High frequency anti-jam
HF ALE	High frequency automatic link establishment
H/W	Hardware
IEEE	Institute of Electrical and Electronic Engineers
IF	Intermediate frequency
INFOSEC	Information Systems Security
I/O	Input/output
IP	Internet protocol
IPT	Integrated product team
ISA	Industry Standard Architecture
ISO	International Standards Organization
ISSE	Information Systems Security Engineering
ISSP	Information Systems Security Policy
JTA	Joint Technical Architecture
JOA	Joint Operational Architecture
kHz	kilo Hertz
LPI	Low probability of intercept
MIB	Management Information Base
Modem	Modulator/demodulator
NTDR	Near Term Digital Radio
NSA	National Security Agency
OA	Operational Architecture
OS	Operating System
PC-104	Embedded-PC Module Standard Consortium
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communication Systems
PMC	PCI Mezzanine Card
PMCS	Programmable Modular Communications System
POSIX	Portable Operating System Interface
PSK	Phase shift keyed
QoS	Quality Of Service
QPSK	Quadrature phase shift keyed

RF	Radio frequency
SA	Systems Architecture
SAE	Society of Automotive Engineers
SATCOM	Satellite communications
SEI	Software Engineering Institute
SEM-E	Standard Electronic Module - E
SINCGARS	Single Channel Ground and Airborne Radio System
SINCGARS SIP	Single Channel Ground and Airborne Radio System Improvement Program
SRM	Systems Reference Model
SWAP	size, weight, and power
SwRM	Software Reference Model
S/W	Software
TA	Technical Architecture
TADIL	Tactical Digital Information Link
TADIX	Tactical Data Information Exchange System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Domain Multiple Access
TOD	Time Of Day
TRANSEC	Transmission security
TRAP/TIBS	Tactical Related Applications/ Tactical Information Broadcast Service
TRIXS	Tactical Reconnaissance Intelligence Exchange System
TX/RX	Transmit/receive
UDP	User Datagram Protocol
UHF	Ultra high frequency
USD (A&T)	Under Secretary of Defense (Acquisition & Technology)
VHF	Very high frequency
VITA	VMEbus International Trade Association
VME	Versa Module Eurocard
VSB	VME Subsystem Bus
WOD	Word Of Day